‘e Scan™

NEW
SLEEK & POWERFUL

Internet Security Suite

Anti-Virus & Content Security

MicroWorld

User’s Guide

The software described in this guide is furnished under a license agreement and may be used only in accordance with the terms of the agreement.

Document Number: 5BDRG/10.18.2010/11.x
Current Software Version: 11.x.x
Copyright Notice: Copyright © 2010. All rights reserved.

Any technical documentation that is made available by MicroWorld is the copyrighted work of MicroWorld and is owned by MicroWorld.

NO WARRANTY: The technical documentation is being delivered to you AS-IS and MicroWorld makes no warranty as to its accuracy or use. Any use of the technical documentation or the information contained therein is at the risk of the user.

Documentation may include technical or other inaccuracies or typographical errors. MicroWorld reserves the right to make changes without prior notice.

No part of this publication may be copied without the express written permission of MicroWorld.

Trademarks: The terms MicroWorld, MicroWorld Logo, eScan, eScan Logo, MWL, MailScan are trademarks of MicroWorld.

To view the eScan Brand Manual, visit the following link.
http://download1.mwti.net/download/New_Artworks/eScan11/BoxShots/brand_manual_eScan_300810.zip

To view the high-resolution box shots for eScan products, visit the following link.
http://download1.mwti.net/download/New_Artworks/eScan11/BoxShots/AV_BOX_JPG.zip

Microsoft, MSN, Windows and Windows Vista are trademarks of the Microsoft group of companies. All product names referenced herein are trademarks or registered trademarks of their respective companies. MicroWorld disclaims proprietary interest in the marks and names of others. Although MicroWorld makes every effort to ensure that this information is accurate, MicroWorld will not be liable for any errors or omission of facts contained herein. MicroWorld reserves the right to modify specifications cited in this document without prior notice.

No part of this document may be reproduced or transmitted in any form or by any means, electronic or mechanical, for any purpose, without the express written permission of MicroWorld.

Other product names mentioned in this manual may be trademarks or registered trademarks of their respective companies and are hereby acknowledged.

Technical Support:	support@escanav.com
Sales:	sales@escanav.com
Forums:	http://forums.escanav.com
eScan Wiki:	http://www.escanav.com/wiki
Live Chat:	http://www.escanav.com/english/livechat.asp
Printed By:	MicroWorld
Date:	October, 2010

Table of Contents

Welcome	3
What Is this Guide All About	4
Overview of eScan's Features	5
Configuring the Test Environment	10
Overview of eScan's Product Installation CD	12
Installing eScan	15
Managing the License Key	24
Verifying the eScan Installation	26
Overview of eScan Protection Center	27
• File Anti-Virus	29
• Mail Anti-Virus	40
• Anti-Spam	54
• Firewall	64
• Scan	73
• Update	78
• Tools	85
• Feedback	89
• Help	89
• Password	90
• License	90
Contact Details	92

Welcome

MicroWorld's eScan 11 is a revolutionary Anti-Virus Software and Information Security product that is designed to provide Zero-Day protection to computers from malicious software and several other security threats.

The new version of eScan is a feature-rich and user-friendly product that comes with several customizable settings. It has a trendy new design that is both intuitive and easy to understand. In addition, eScan 11 introduces a host of new features that are aimed at safeguarding your computer from new and emerging threats such as malware; phishing Web sites and e-mails; and hackers. To achieve this, eScan employs cutting-edge technologies, such as MicroWorld Winsock Layer (MWL), Non Intrusive Learning Patterns (NILP), and Domain IP Reputation Check (DIRC).

MicroWorld is committed to provide a safe and secure computing environment for all eScan users. This guide is designed to help you use/evaluate the features and tools included in eScan 11.

Thank you for choosing eScan.

The eScan Team

What Is this Guide All About?

Over the past few years, several new software technologies have come into existence. With their advent, the number of security threats in the computing world has grown exponentially. As a result, individuals and organizations have started raising concerns about the security of their data and personal information.

This self-explanatory guide contains detailed information on eScan Anti-Virus (AV) version 11.x.x. It is targeted at users, customers, software testers, and individual users and aims at helping them use the product efficiently and effectively.

This guide is organized into three main sections: the first section provides an overview of the new and enhanced features in eScan 11, the next section deals with the various elements of eScan's graphical user interface (GUI), and the last section discusses each modules of eScan 11 in detail. These sections include detailed instructions and screen shots, where necessary.

For any queries regarding eScan, please write to **support@escanav.com.**

To contact our support team via Live Chat, please visit the following link.
http://www.escanav.com/english/livechat.asp.

Overview of eScan's Features

eScan epitomizes the next generation of Anti-Virus software products that handle security threats from a new dimension without compromising the performance of your computer. It uses powerful technologies such as the MicroWorld Winsock Layer (MWL) technology, Domain and IP Reputation Checker (DIRC) technology, Non Intrusive Learning Pattern (NILP) technology, and sophisticated Heuristics Algorithms to detect and clean malware. In addition, it includes a comprehensive set of powerful management tools, such as the eScan Management Console (EMC) and eScan Protection Center (ePC). These tools help you configure eScan to safeguard your data and computers based on your requirements.

New Features in eScan 11

eScan 11 includes several improvements over its predecessor in terms of its user interface, performance, resource utilization, and data protection features. These new features are described as follows:

- **New Trendy GUI**

  eScan 11 has a trendy new GUI that is extremely simple and easy to use. It is elegant in terms of its design and is well suited to the needs of both expert and novice users. The new GUI is extremely light on system resources and requires very less memory space to run efficiently. It thus provides the user with a secure and pleasant computing experience without compromising on the performance of the computer.

- **Product Installation CD with Bootable Rescue Disk**

  eScan 11's product installation CD comes with a set of installation setup files and a bootable Rescue Disk. The bootable Rescue Disk enables the user to clean boot the computer if the operating system fails to load on it. When the user boots the computer by using the Rescue Disk, the eScan Anti-Virus Toolkit (formerly MWAV) scans and cleans the computer's memory, registry, startup folders, system folders, and drives of viruses and spyware.

- **Gaming Mode**

  eScan 11 includes a Gaming Mode, which provides an uninterrupted gaming experience to users while they are running gaming applications in the full screen

mode. The benefit of the Gaming Mode lies in how eScan handles alerts while a user is playing a game. Normally, when a user switches on a computer running eScan, the real-time protection module starts running in the background. Now, when a user starts a game, eScan may display alerts and notifications, which may affect the user's game. The Gaming Mode in eScan 11 has been designed to overcome this problem. Whenever a user runs a game on a computer, eScan 11 automatically enables the Gaming Mode, which prevents alerts and notifications from being displayed. eScan automatically disables this mode when the user exits the gaming application. Thus, the Gaming Mode provides the user with an uninterrupted and seamless gaming experience.

Note: The USB password protection module will remain active even while the Gaming Mode is on. Also, in the Gaming Mode, updates that are downloaded will not reflect in the eScan database.

❑ Automatic Detection of Laptop Mode

eScan 11 includes the automatic detection of Laptop Mode feature, which is a power-saving feature that provides unmitigated battery time for laptops.. Whenever a user switches to the Laptop Mode, eScan 11 automatically detects this change and prevents memory intensive processes like scheduled scans from running. Note that eScan's real-time protection remains active while the laptop is in the Laptop Mode.

❑ Virtual Keyboard

eScan 11 provides users with a Virtual Keyboard that helps them avoid using their keyboard to enter confidential information. This is highly useful because it has several security benefits. Malware writers create malware because of their need to obtain a payload. The payload for a password-stealing Trojan may be the authentication information of a user's online banking account. Malware often include keyloggers, which are programs designed to capture the keystrokes on the computer on which they are installed. Whenever a user fills in details such as user name or password on an online form, the keylogger obtains this information and then sends it to the hacker. The user interface of eScan's Virtual Keyboard simulates the user's keyboard and acts as a secure mechanism for the user to enter sensitive information, such as credit card details and banking passwords, without any fear of data theft due to keyloggers.

❑ Enhanced Self Protection

eScan 11 comes with the enhanced Self Protection feature that protects critical eScan files and folders from being deleted or modified. Some new generation malware try to infect computers by deactivating the Anti-Virus software running on them. They try to achieve this by either disabling the Anti-Virus software or by deleting critical files that are necessary for running the Anti-Virus software. The enhanced Self Protection feature of eScan 11 prevents malware from either disabling eScan or deleting its critical files thus keeps computers safe from infections. The feature protects eScan services such as eScan updater, eScan server, and MailScan Dispatcher from being stopped and/or terminated. It also protects eScan executables or services running in the memory from being stopped and/or terminated.

❑ Malicious URL Filtering

This feature of eScan 11 blocks suspicious URLs. It thus prevents users or malware from accessing URLs, which are already found to be infected and harmful to the computer.

❑ Folder Protection

eScan 11 includes the new Folder Protection feature. This feature helps users protect specific files and folders from being modified or deleted. The main advantage of this feature is that it prevents the specified files from being infected by malicious software. Another advantage of this feature is that files and folders that are protected cannot be deleted unless the folder protection is turned off. This helps users safeguard their confidential data from infections by malware and accidental deletions.

❑ Automatic Patching of Windows® Operating System Vulnerabilities

eScan 11 automatically checks the Microsoft® Web site and downloads critical hotfixes and updates for the Windows® operating systems as and when they become available. Most new strains of malicious software, such as Rootkit.Stuxnet.A and Rootkit.TmpHider exploit the vulnerabilities in operating systems. eScan 11 ensures that the computer on which it is installed has the latest hotfixes and updates installed on it. Thus, eScan prevents malicious software that

exploit vulnerabilities in the operating system from infecting the computer and helps users protect their data from hackers and other security threats.

Enhanced Features

eScan 11 includes several features that were a part of eScan 10. The enhanced features are as follows:

- **Anti-Virus Engine:** This engine is an intelligent malware-detection engine that finds and cleans malicious software on the fly.
- **Heuristic Scan Engine:** This engine detects unknown malicious software.
- **Block Spam:** This feature helps you block unsolicited e-mails from reaching your inbox.
- **Block Attachment:** This feature helps you specify e-mail attachment types that eScan should block automatically.
- **Proactive Security:** This feature prevents unknown or suspicious applications from executing and compromising the security your computer.
- **Firewall:** This feature prevents unauthorized access to or from any network. It also includes the Network Traffic Monitor, which provides a graphical representation of the incoming and outgoing network traffic on a real-time basis.
- **Auto-download Updates:** This feature automatically downloads free updates from eScan update servers.
- **Windows®-based Rescue Disk:** This feature helps you create a bootable rescue CD that could be used to remove sophisticated rootkit infections that do not allow the anti-virus software to remove the infections when the computer is booted in regular mode.
- **eScan Remote Support:** This feature helps you request the assistance of an eScan Technical Support Representative through a remote connection to your computer. It allows the eScan Technical Support Representative to remotely take control and troubleshoot the eScan-related issues on your computer.
- **eScan Auto-backup and Restore:** This feature helps you back up the critical files of the Windows® operating system installed on your computer. It then automatically restores the clean files when eScan finds an infection in any of the system files that cannot be disinfected.
- **Download Latest Microsoft® Operating System Hotfix:** This feature downloads critical patches and hotfixes for the Windows® operating system.

To view the eScan product-comparison sheet, visit the following link.

http://escanav.com/documents/escan11/eScan_product_comparison.asp

Note: Depending on the product, some of the listed features may be unavailable.

Configuring the Test Environment

This section provides you with information on configuring a test environment for using eScan.

Software Requirements

eScan products (for the Small Office Home Office [SOHO] segment) run on the 32-bit or 64-bit editions of following operating systems. Your computer should have any one of the following operating systems installed on it.

- Windows® 2000 SP4 with KB891861
- Windows® XP Professional with SP2 and above (For 32-bit edition only)
- Windows® XP with SP1 and above (For 64-bit edition only)
- Windows® Vista Ultimate
- Windows® Vista Home Premium
- Windows® Vista Home Basic
- Windows® Vista Business
- Windows® Vista Enterprise
- Windows® 7 Ultimate
- Windows® 7 Home Premium
- Windows® 7 Home Basic
- Windows® 7 Business
- Windows® 7 Enterprise

In addition, it requires a PDF reader and Internet Explorer® version 5.0 or higher installed on the computer.

Note: The SOHO product will not work on server-based operating systems.

Minimum Hardware Requirements

Your computer must meet the following minimum requirements.

- Processor: Pentium II 200 MHz
- RAM: 256 Megabytes (MB) of RAM (recommended 512 MB)
- Hard Disk Space: 700 MB of free hard disk space
- Additional Drives: CD-ROM drive

Preinstallation Steps

Before installing eScan, please ensure that you perform the following tasks.

- **For First-time Installation**

  - Ensure that you have administrator rights or equivalent privileges for the user logged on to the computer.
  - Close all the open applications or programs.
  - Uninstall all other Anti-Virus or Anti-Spyware software.
  - Disable or uninstall Windows® Defender.
  - Disable or uninstall any existing firewall software, including Windows® Firewall.
  - Determine the largest free drive or partition and then install eScan on it.
  - Additional tasks:

    - **Recommended:** MicroWorld recommends that the computer on which eScan is being installed is connected to the Internet during the installation process. This will ensure that eScan downloads all the latest updates from eScan update servers.
    - **Optional:** Ensure that you know the IP address of the mail server to which eScan should send warning messages. If authentication for the mail server is mandatory for accepting e-mails, you will need authentication user name and password to send e-mails.
    - **Optional:** Ensure that the critical operating system and security patches are installed on the computer.

- **For Renewal or Upgrade Installation**

  - You should perform the same set of tasks that were performed while installing eScan for the first time. Then, you can upgrade to the newer version without uninstalling the existing version.

- **For Reinstalling After Uninstalling the Existing Version**

  - If you have uninstalled an existing version of eScan, you must restart the computer before you can reinstall it.

Overview of eScan's Product Installation CD

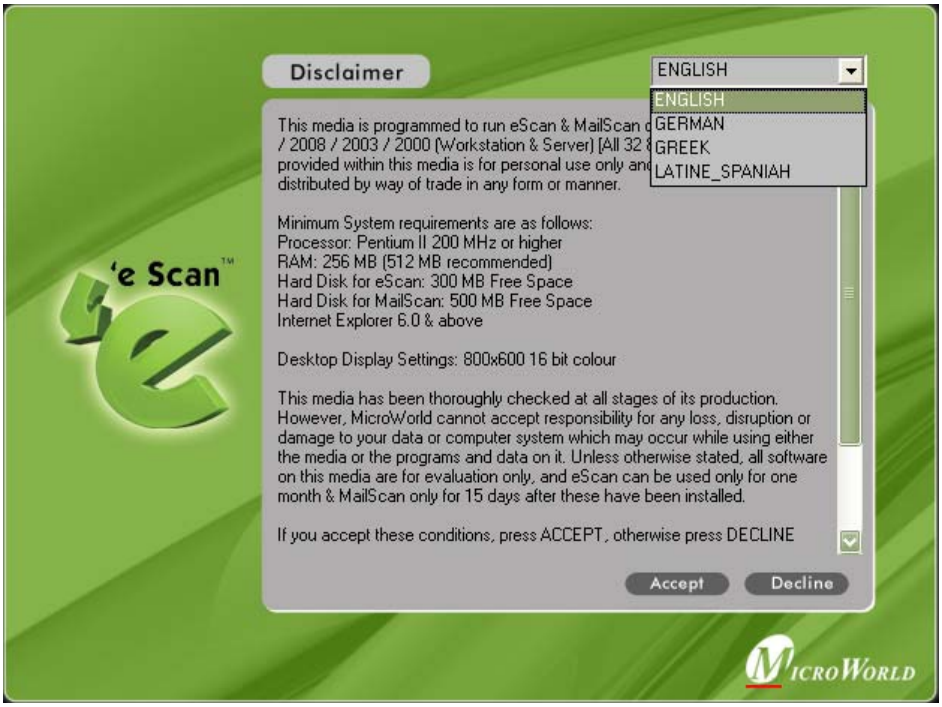
The eScan product installation CD comes with a set of installation setup files and a bootable Rescue Disk. You can use the bootable Rescue Disk to boot your computer if the operating system cannot be loaded.

The Rescue Disk also includes the eScan Anti-Virus Toolkit (formerly MWAV), which runs automatically when you boot the computer using the disk. It helps you scan the computer's memory, registry, startup folders, system folders, and drives for viruses and spyware. In addition, it helps you run the Command.exe file and execute commands for formatting the hard disk, partitioning any drive, or checking the hard disk for errors.

Note: When you boot from Rescue Disk, the updates download by MWAV will be stored on the local hard-drive and not in the memory.

The eScan product installation CD contains an AUTORUN.exe file. You can view the contents of the CD and install eScan by using this CD.

When you double-click AUTORUN.exe, the Disclaimer is displayed. You can either accept the disclaimer to view the CD's menu or decline it to exit the screen.


Disclaimer
ENGLISH
ENGLISH
GERMAN
GREEK
LATINE_SPANIAH
This media is programmed to run eScan & MailScan
/ 2008 / 2003 / 2000 (Workstation & Server) (All 32
provided within this media is for personal use only an
distributed by way of trade in any form or manner.
Minimum System requirements are as follows:
Processor: Pentium II 200 MHz or higher
RAM: 256 MB (512 MB recommended)
Hard Disk for eScan: 300 MB Free Space
Hard Disk for MailScan: 500 MB Free Space
Internet Explorer 6.0 & above
Desktop Display Settings: 800x600 16 bit colour
This media has been thoroughly checked at all stages of its production. However, MicroWorld cannot accept responsibility for any loss, disruption or damage to your data or computer system which may occur while using either the media or the programs and data on it. Unless otherwise stated, all software on this media are for evaluation only, and eScan can be used only for one month & MailScan only for 15 days after these have been installed.
If you accept these conditions, press ACCEPT, otherwise press DECLINE
Accept
Decline
'e Scan
MicroWorld

Disclaimer

The CD's menu shows the following options.

- **Scan My System:** You can click this button to scan your computer for viruses and other malware by using the eScan Anti-Virus Toolkit.
- **Products:** You can click this button to view information about eScan or install it on your computer.
  Note: You can click the **Info** button to view the Quick Reference Guide for eScan in the .PDF format.

Autorun Menu

- **Browse CD:** You can click this button to view the contents of the CD.
- **Visit Web site:** **[Requires Internet connectivity.]** You can click this button to visit the eScan Web site i.e., **http://www.escanav.com**.
- **Contact Us:** You can click this button to view the contact information for MicroWorld's offices.

Additional Requirements

1. Internet connectivity is required for a few buttons to function properly.

Installing eScan

You can install eScan Anti-Virus (AV) either by using the eScan setup file or by using the eScan product installation CD.

To download the eScan setup file, visit the following link.
http://www.escanav.com/downloads/soho11.asp

To begin the eScan installation, insert the eScan product installation CD into the CD-ROM drive of your computer. This will start the setup automatically.

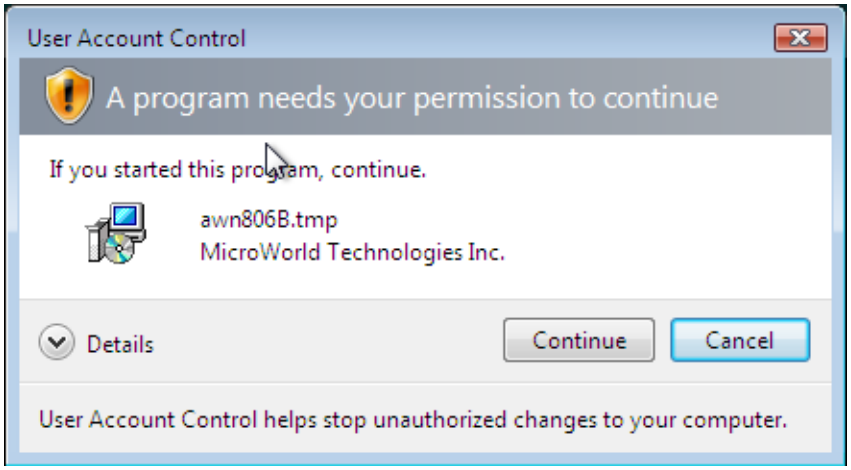
Some computers do not play the eScan product installation CD automatically. In such cases, you can manually start the installation by double-clicking the AUTORUN.exe in the CD-ROM drive window. This will display a dialog box containing options for selecting the language.

eScan uses the Interactive Installation Wizard for its installation. This wizard has a simple and intuitive GUI that guides you through the installation process.

Installation Steps

To install eScan AV on your computer, perform the following steps.

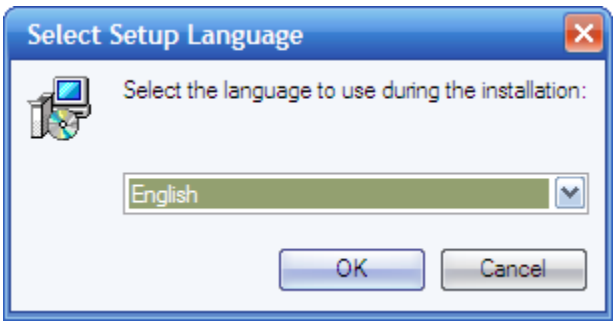
Special instructions for Installing eScan AV on computers running the Windows Vista® operating system with User Access Control (UAC) enabled on them.
When you double-click the setup file for installing eScan AV, a User Access Control message box asking you for permission to run a awn2[*xxxx*].tmp file is displayed. Here, the [*xxxx*] represents the last four characters, which may be arbitrary. This is a valid eScan file. To proceed with the installation, click **Continue**.



User Account Control message box

STEP 1 – Choosing the Language

eScan AV is available in many languages, such as English, German, French, Nederlands, Italiano, Portuguese, Spanish, Turkish, Chinese Simplified, Chinese Traditional, Greek, Korean, Norwegian, Russian, Polish, and Latin Spanish.

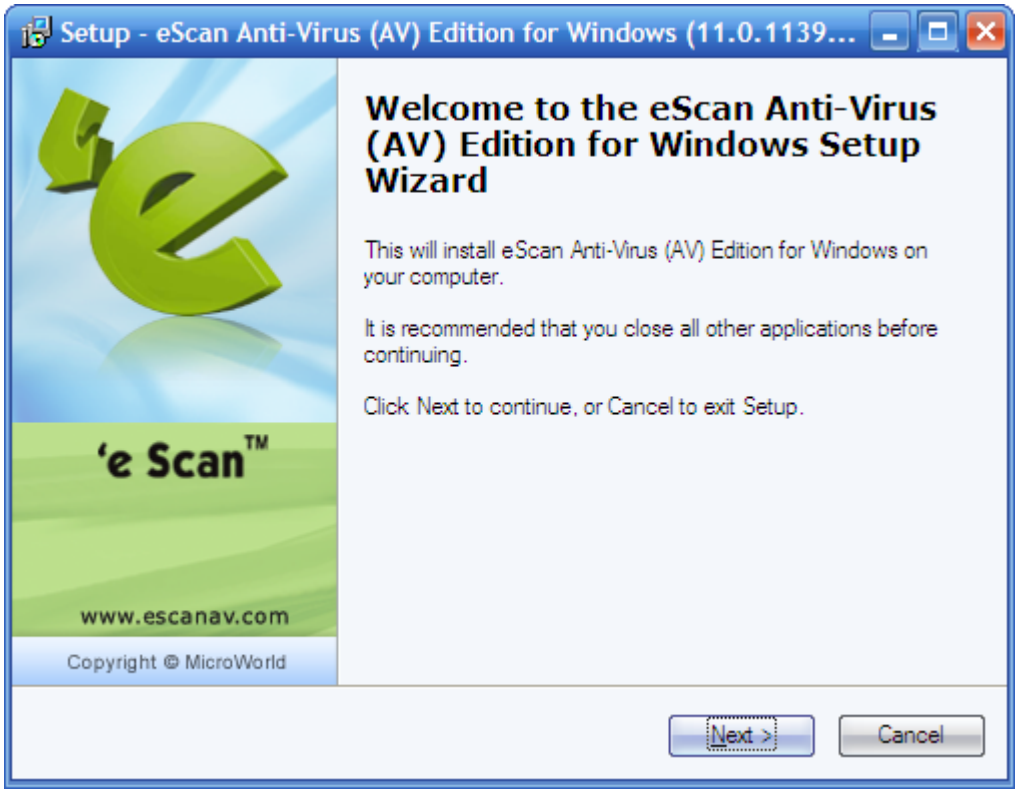


Selecting the Language

Select the preferred language from the drop down list, and then click **OK**.

STEP 2 - Installation Wizard Welcome Screen

The welcome screen helps you decide whether you want to proceed with the installation of eScan.


Setup - eScan Anti-Virus (AV) Edition for Windows (11.0.1139...
Welcome to the eScan Anti-Virus (AV) Edition for Windows Setup Wizard
This will install eScan Anti-Virus (AV) Edition for Windows on your computer.
It is recommended that you close all other applications before continuing.
Click Next to continue, or Cancel to exit Setup.
'e Scan™
www.escanav.com
Copyright © MicroWorld
Next >
Cancel

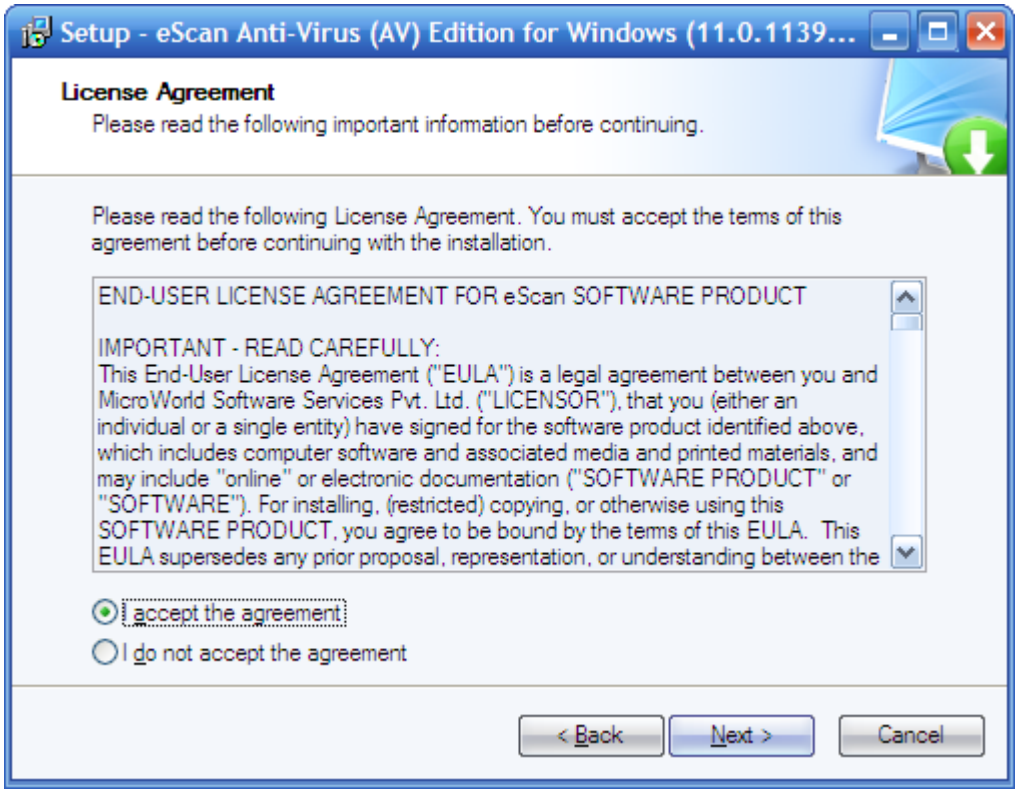
Welcome Screen

To proceed with the installation, click **Next**. This will display the **License Agreement** screen.

Alternatively, if you do not wish to proceed, you can click **Cancel**. This will cancel the installation and close the wizard.

STEP 3 - License Agreement
This screen displays the EULA for eScan. Please read it carefully.

To accept the EULA, on the **License Agreement** screen, click **I accept the agreement**, and then click **Next**. This will display the **Select Destination Location** screen.


Setup - eScan Anti-Virus (AV) Edition for Windows (11.0.1139...
License Agreement
Please read the following important information before continuing.
Please read the following License Agreement. You must accept the terms of this agreement before continuing with the installation.
END-USER LICENSE AGREEMENT FOR eScan SOFTWARE PRODUCT
IMPORTANT - READ CAREFULLY:
This End-User License Agreement ("EULA") is a legal agreement between you and MicroWorld Software Services Pvt. Ltd. ("LICENSOR"), that you (either an individual or a single entity) have signed for the software product identified above, which includes computer software and associated media and printed materials, and may include "online" or electronic documentation ("SOFTWARE PRODUCT" or "SOFTWARE"). For installing, (restricted) copying, or otherwise using this SOFTWARE PRODUCT, you agree to be bound by the terms of this EULA. This EULA supersedes any prior proposal, representation, or understanding between the
I accept the agreement
I do not accept the agreement
< Back
Next >
Cancel

EULA

Alternatively, if you do not wish to accept the EULA, you can click **Cancel**. This will cancel the installation and close the wizard.

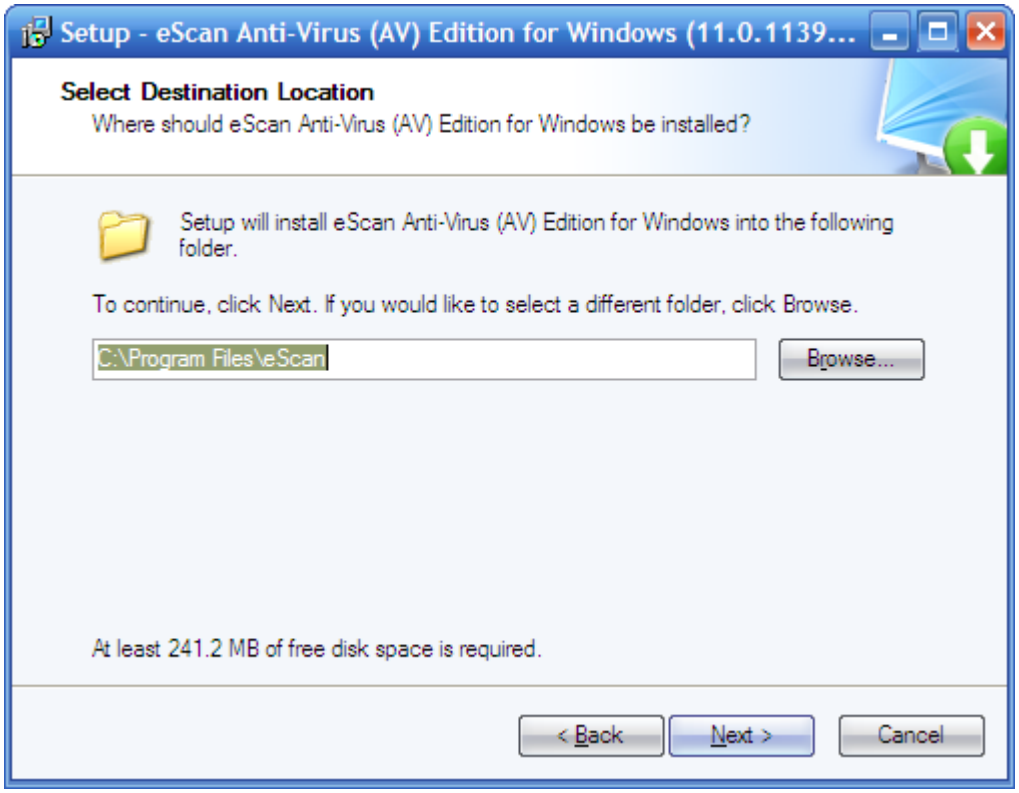
STEP 4 - Selecting the Installation Folder

In this step, you can select the drive and folder in which you want to install eScan.

To select the eScan installation folder on your computer, on the **Select Destination Location** screen, in the box, either type the path of the folder or click **Browse** to browse to the folder, and then click **Next**.

Note:

- The default path for 32-bit computer: ***[Disk Drive]*\Program Files\eScan**
- The default path for 64-bit computers: ***[Disk Drive]*\Program Files (x86)\eScan**


Setup - eScan Anti-Virus (AV) Edition for Windows (11.0.1139...
Select Destination Location
Where should eScan Anti-Virus (AV) Edition for Windows be installed?
Setup will install eScan Anti-Virus (AV) Edition for Windows into the following folder.
To continue, click Next. If you would like to select a different folder, click Browse.
C:\Program Files\eScan
Browse...
At least 241.2 MB of free disk space is required.
< Back
Next >
Cancel

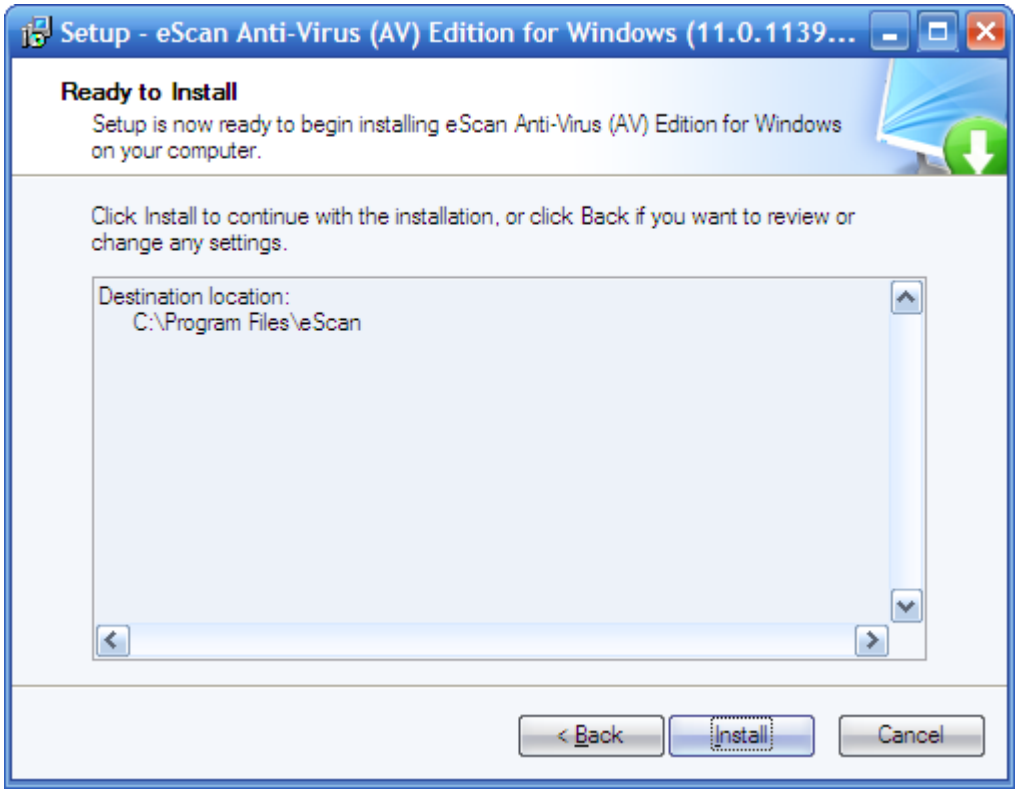
Welcome Screen

Alternatively, if you need to view the EULA, you can click **Back** to navigate to the **License Agreement** screen.

However, if you do not wish to proceed, you can click **Cancel**. This will cancel the installation and close the wizard.

STEP 5 – Viewing the Summary Report Before Installation

This window shows a summary of the options that you have selected on the previous screens of the wizard. This step completes the preparation for installing the application on your computer. You can click the **Back** button to review or change the settings that you have made on the previous screens.


Setup - eScan Anti-Virus (AV) Edition for Windows (11.0.1139...
Ready to Install
Setup is now ready to begin installing eScan Anti-Virus (AV) Edition for Windows on your computer.
Click Install to continue with the installation, or click Back if you want to review or change any settings.
Destination location:
C:\Program Files\eScan
< Back
Install
Cancel

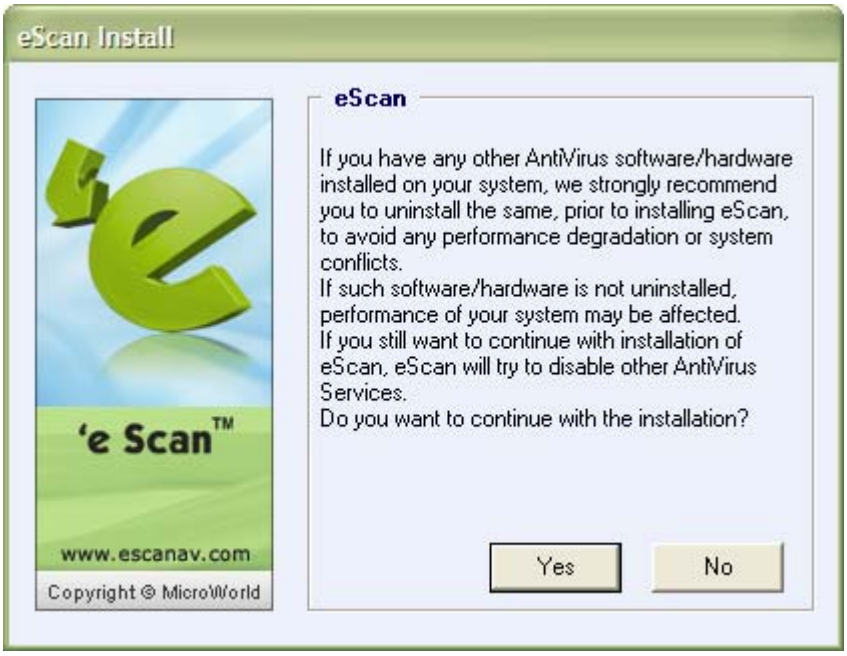
Summary Report

To proceed with the installation, click **Install**. When you click Install, the wizard should start installing eScan on the computer.

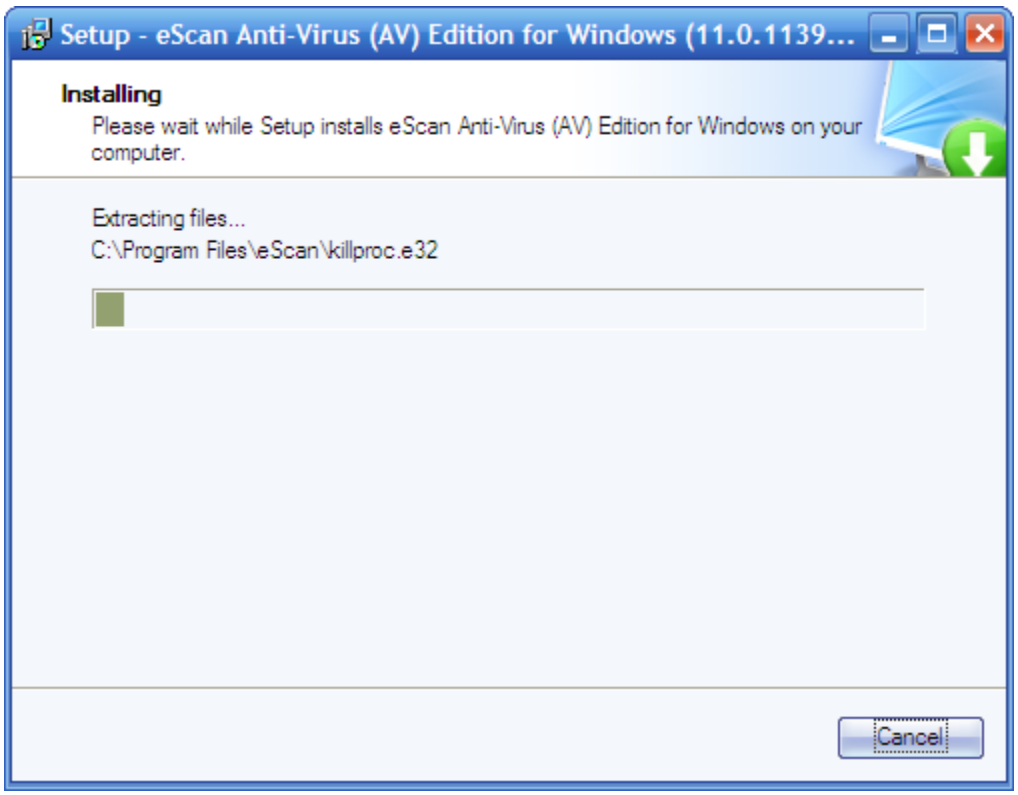
However, if you do not wish to proceed, you can cancel the installation by clicking **Cancel**.

STEP 6 – Install eScan

During the installation process, the wizard searches your computer for other Anti-Virus programs that may conflict with the eScan installation and prompts you to remove them. If there are no conflicting programs, the wizard proceeds with the installation.


eScan Install
eScan
'e Scan™
www.escanav.com
Copyright © MicroWorld
If you have any other AntiVirus software/hardware installed on your system, we strongly recommend you to uninstall the same, prior to installing eScan, to avoid any performance degradation or system conflicts.
If such software/hardware is not uninstalled, performance of your system may be affected.
If you still want to continue with installation of eScan, eScan will try to disable other AntiVirus Services.
Do you want to continue with the installation?
Yes
No

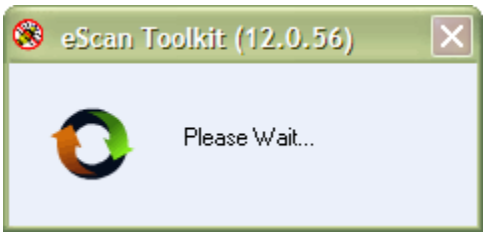
eScan Installation Confirmation


Setup - eScan Anti-Virus (AV) Edition for Windows (11.0.1139...
Installing
Please wait while Setup installs eScan Anti-Virus (AV) Edition for Windows on your computer.
Extracting files...
C:\Program Files\eScan\killproc.e32
Cancel

Installing eScan

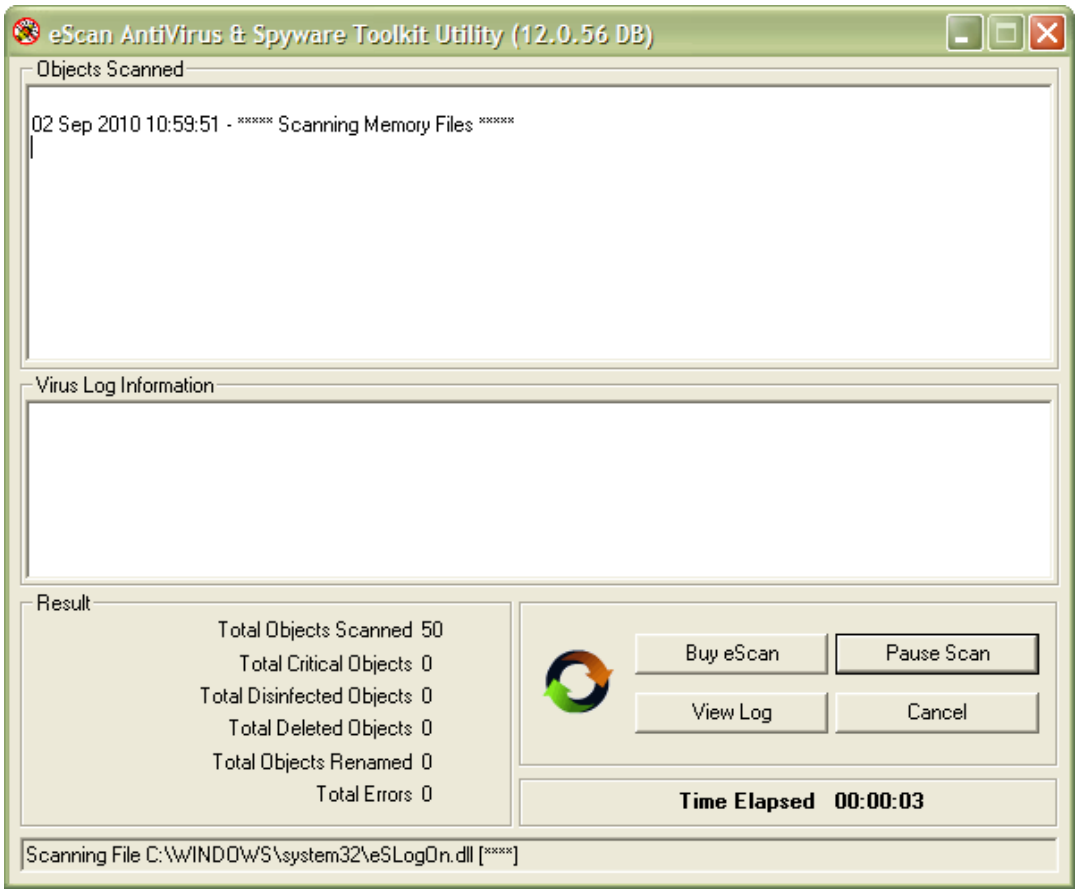
Installing eScan

If you do not wish to proceed, you can cancel the installation by clicking **Cancel**.



MWAV initialization

The eScan setup also runs eScan Anti-Virus Toolkit. This tool scans and removes the viruses and spyware found on your computer.



eScan Anti-Virus Toolkit

STEP 7 - Completing the Installation

Next, the eScan Install screen is displayed and the icon shows up in the notification area of the task bar.

To complete the installation of eScan and restart your computer, on the **eScan Install** screen, click **Yes**.

Confirmation Screen

You can also choose to restart your computer later by clicking **No**. In this case, eScan completes the installation without restarting your computer and then displays the **Installation Completion** screen.

eScan Installation (Continued)

The **Installation Completio**n screen provides you with options for restarting your computer either immediately or later. To complete the installation of eScan and restart your computer, on the **Installation Completion** screen, click **Yes, restart the computer now**, and then click **Finish**. This will restart your computer immediately.

Setup - eScan Anti-Virus (AV) Edition for Windows (11.0.1139...
Completing the eScan Anti-Virus (AV) Edition for Windows Setup Wizard
To complete the installation of eScan Anti-Virus (AV) Edition for Windows, Setup must restart your computer. Would you like to restart now?
Yes, restart the computer now
No, I will restart the computer later
'e Scan™
www.escanav.com
Copyright © MicroWorld
Finish

Installation Completion Screen

Note: The **Yes, restart the computer now** option is selected by default.

Alternatively, you can choose to restart your computer later by clicking **No, I will restart the computer later**, and then clicking **Finish**. The installation wizard will close without displaying any message.

Note:

- When you enter the new 30-character license key that you have received after purchasing or renewing the eScan license, ensure that there are no spaces before, in between, or after the characters in the key. For example: **ABCD-EFGH-ABCD-EFGH-ABCD-EFGH-ABCD-EF**
- After entering the key, click **Apply**, and then click **OK**.

Adding the Standard License Key

1. Click **Start**, point to **All Programs**, point to **eScan for Windows, and then click eScan Registration**.
2. In the License Information window, in the **Enter License Key** box, enter the 30-character license key in capital letters, and then click **Apply**.
3. In the **Confirmation** message box, click **OK**.

Activating the License Key

1. In the License Information window, select the license key that you have just entered, and then click **Activate Now**. Alternatively, you can right-click the license key displayed under the **Standard Key (30 char)** tab, and then click **Activate Now**.
2. Ensure that the **Activate Now** option is selected, and then click **OK**.
   Note: If you have received the eScan Activation code via an e-mail from register@escanav.com, you can select **I have Activation Code**. In this case, copy the activation code, and then paste it in the **Enter Activation Code** box.
3. Provide your personal information, and then click **Next**.
   Note: **E-mail ID (Address)** and **Purchased From** are the only mandatory fields that you have to fill. If you do not want to disclose any other personal information, you can leave the other fields blank.
4. In the next window, you will have three options to register your copy of eScan: **Online**, **Fax**, and **E-mail**.

   - If you are activating eScan by using the Online method, ensure your computer is connected to the Internet, and then click **Activate**. A new 51-character key

will be automatically added to the License Information window and your copy of eScan will be activated.

- If the Online method fails, you could either activate eScan via the E-mail or Fax methods. Select either the **E-mail** option or the **Fax** option, and then click **Activate**. Offline activations via the e-mail method or the Fax method may take up to 48 hours to process. If you opt for the e-mail method, please ensure that you send the e-mail to **register@escanav.com**.
- The Fax method will output a FaxRegister.TXT file, which you can print and fax to the nearest MicroWorld office.

  To view the fax numbers of all MicroWorld offices, visit the following Web page.
  http://www.escanav.com/contactus.asp

  You can also save the FaxRegister.TXT file and e-mail it to **register@escanav.com**.
  OR
  You can activate your standard key through the eScan Web site using the following link.
  http://www.escanav.com/Websiteactivation

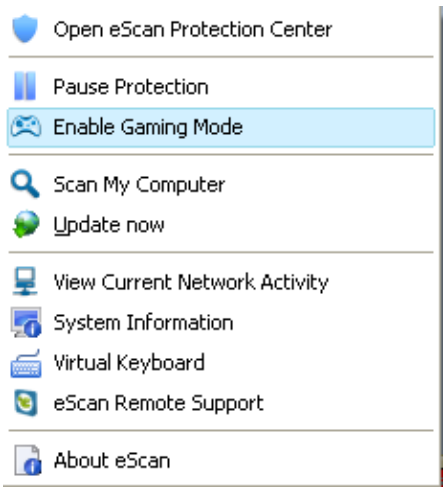
  For more information on how to register your copy of eScan, read the *Know how to register your product* article on the following Web page.
  http://www.escanav.com/register

  After you receive the Activation Code either by fax or by e-mail, perform the steps in *Activating the License Key* from Step 2 onwards.

Verifying the eScan Installation

When the installation is complete, a red shield icon appears in the system tray. The shield icon indicates the protection status of the computer. If the icon has a cross mark , it indicates that eScan's real-time protection is paused or disabled, otherwise without the cross mark it means that the real-time protection is active.

You can find the version of eScan installed on your computer by placing the mouse pointer on . In addition, you can right-click on it to view a context menu. This menu contains options for scanning the computer, downloading updates, pausing eScan's real-time protection, and some tools for optimizing the system performance.



Context Menu

You can access eScan Protection Center by either clicking . Alternatively, you can open the eScan Protection center by right-clicking and then clicking **Open eScan Protection Center**. However, before you can access this window, you need to specify the Administrator password if it has been set. The default Administrator password for eScan Protection Center is **admin**. As a best practice, for additional security, you should change the password, after you install eScan.

The Administrator Password window also contains a **Read Only** button. You should click this button if you need to prevent changes or modifications from being made to the settings. This mode enables users to access eScan Protection Center in the restricted or read-only mode.

Overview of Scan Protection Center

eScan Protection Center is the main application window of eScan. It has a new GUI that is pleasantly straightforward and is designed to suit the needs of both novice and expert users.

eScan Protection Center

In addition, it provides quick access to the following feature settings.

- **Protection:** The GUI uses docking view for displaying the icons representing the modules of the Protection feature. You can click the individual docking icons to access the protection status settings for the File Anti-Virus, Mail Anti-Virus, Anti-Spam, and Firewall modules. Out of these, the Mail Anti-Virus and Anti-Spam modules are disabled by default.

Icons in the Docking View

- **File Anti-Virus:** This module provides real-time protection to the files and folders residing on your computer.
- **Mail Anti-Virus:** This module prevents infected e-mails and attachments from reaching your inbox, and thus protects your computer from malicious programs that propagate through e-mails.
- **Anti-Spam:** This module helps you create and configure filters that filter spam based on keywords and phrases that appear within e-mails.
- **Firewall:** This module helps you apply various expert rules for blocking specific ports, programs, or services on your computer.

- **Scan:** You can click this button to configure scheduled scans or run on-demand scans.

Additional eScan Modules

- **Update:** You can click this button to configure daily updates. However, to download the latest updates, your computer needs to be connected to the Internet.
- **Tools:** You can click this button to access the tools available in eScan.

Note: Whenever you click any of the buttons or icons listed above, a tabbed page containing settings related to that module is displayed.

The right-hand side top corner of the eScan Protection Center window provides you with access to the following modules.

- **Feedback:** You can click this button to visit the eScan Web site where you can provide your feedback and send it to the eScan's Quality Assurance team.
- **Help:** You can click this button to view for the online technical help on eScan. However, this requires your computer to be connected to the Internet.
- **Password:** You can click this button to change the Administrator password for eScan Protection Center.
- **License Information:** You can click this button to register and activate the license key.

Depending on whether a module is running or stopped, the icons in the Protection module show the following status icons.

- Tick-marked icons indicate that the module is running.
- Cross-marked icons indicate the module is stopped or turned off.

When you select an icon, the tabbed page shows you some information regarding the selected module. It also provides you with buttons for configuring that module and helps you view reports generated by eScan for that module. With the exception of Scan and Tools, the tabbed pages belonging to all other modules show the following information.

- **Configuration:** This is the first section displayed in the tabbed page of each module. This section displays the status of the module, whether it is running or not. In addition, the eScan Protection Center window shows the following buttons when an icon is clicked in the docking view.
    - **Start:** You can click this button to start a particular module.
    - **Stop:** You can click this button to stop a particular module.
    - **Settings:** You can click this button to open the application's configuration window.
- **Reports:** This pane helps you view the reports generated by the corresponding module. The Scan module and the Tools module do not show the Reports section.

File Anti-Virus

File Anti-Virus is a part of the eScan's Protection feature. This module monitors and safeguards your computer on a real-time basis from all kinds of malicious software as files are accessed, copied, or executed. This module includes the Proactive Scanning feature, which helps you blocking applications that perform suspicious activities. File Anti-Virus also includes the Block Files feature. This feature allows you to block or quarantine files from being accessed from local or network drives. In addition, File Anti-Virus also allows you to enable Folder Protection, which prevents users from creating, deleting, or updating files or subfolders within specified folders.

File Anti-Virus

When you click the File Anti-Virus icon in the docking view of eScan Protection Center, the tabbed page for the File Anti-Virus module is displayed. The tabbed page contains information about the status of the module, settings, and buttons for displaying the recent scans performed by the module. This page has two sections: **Configuration** and **Reports**, both of which are described as follows:

❑ Configuration

This section provides you with information regarding the status of File Anti-Virus and Proactive Scan. It also shows you the default action that File Anti-Virus will perform when it detects a malicious program.

This section displays the following information.

- **File Anti-Virus Status:** It shows whether File Anti-Virus is running or not.
- **Proactive Scan Status:** It displays whether proactive scanning is enabled or not.
- **Action:** It shows the action that eScan will perform when a malicious program is detected by File Anti-Virus.

The page also displays the following buttons.

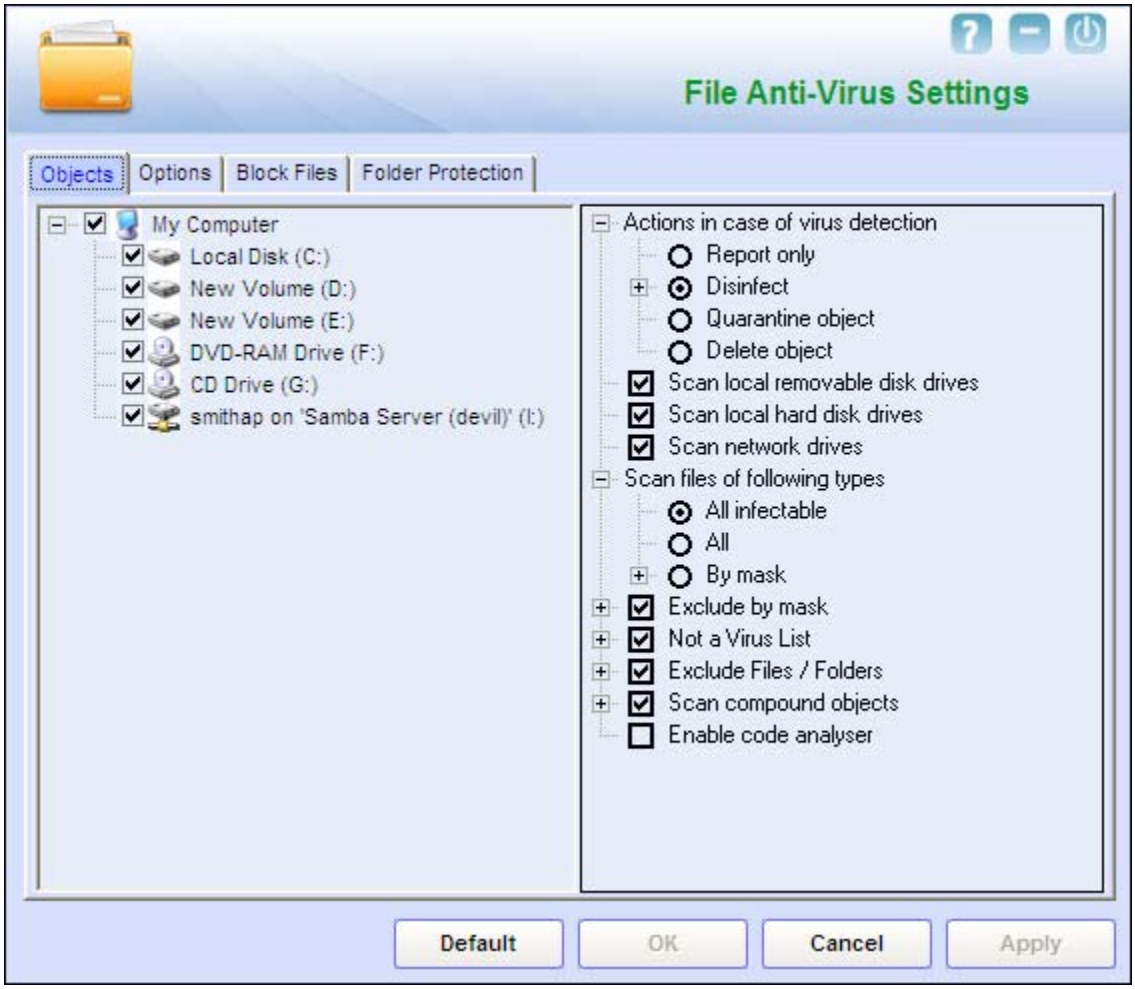
- **Start/Stop:** This button is a toggle button. You can click this button to switch File Anti-Virus easily from the start state to the stop state and vice versa.
- **Settings:** This button opens the **File Anti-Virus Settings** dialog box, which helps you configure the File Anti-Virus module for real-time monitoring. This dialog box has two tabs: **Objects** and **Options,** which are described as follows:

1. Objects

This tab displays the available drives on the computer. It allows you to configure the actions that File Anti-Virus should perform when it encounters a security threat during the scan operation.

This tab is divided into two panes; they are described as follows.

- **The left pane:** This pane displays all the removable and non-removable drives, network drives, installed drives, and mapped drives that File Anti-Virus can monitor or scan. All the drives displayed on the left pane are selected by default.



The Objects Tab

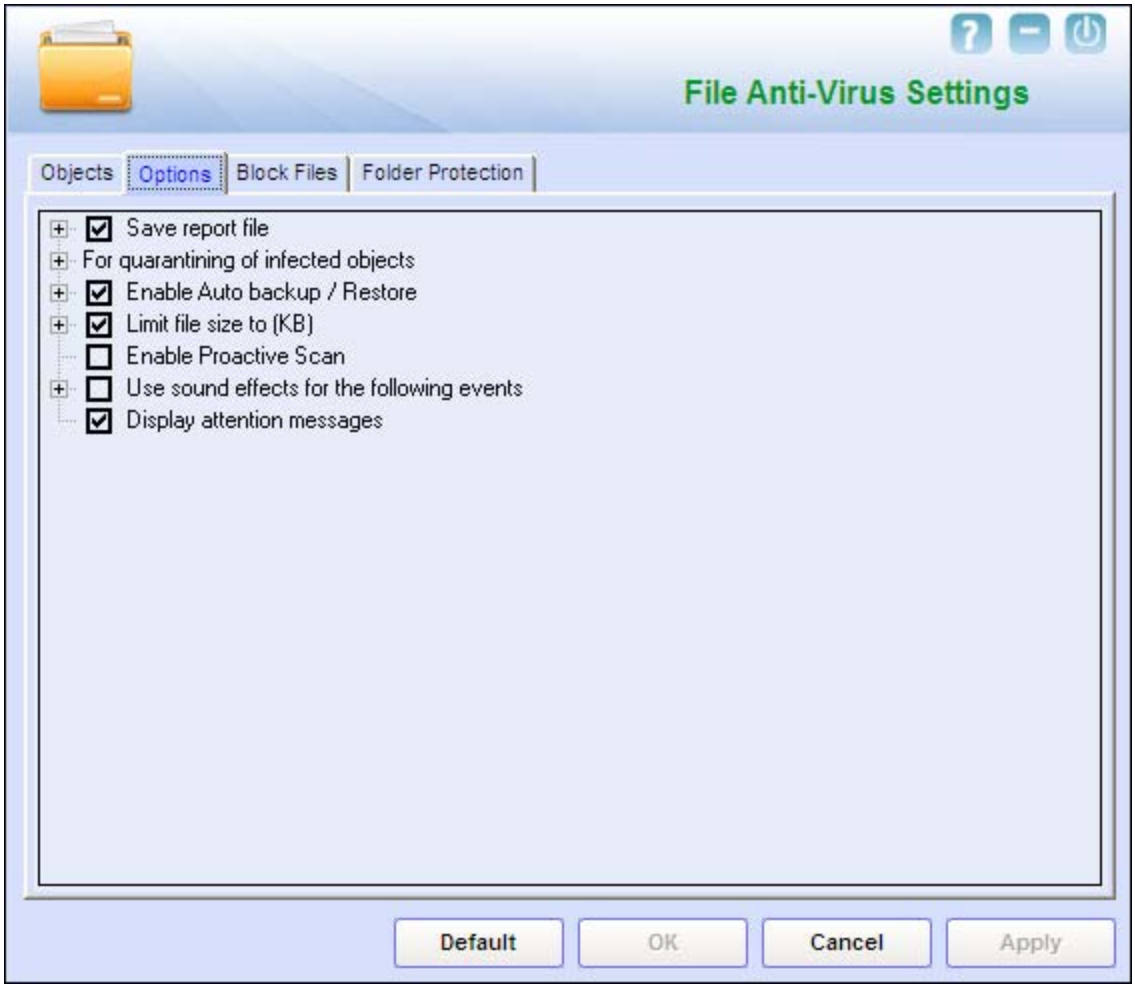
- **The right pane:** This pane provides you with a number of settings for fine-tuning the File Anti-Virus module as per your requirements. For example, you can configure module to scan specific storage devices or exclude files of a given file type.

  - Actions in case of virus detection: This section lists the different actions that File Anti-Virus can perform when it detects a virus infection. These actions are Report only, Disinfect, Quarantine, and Delete object. Out of these, the **Disinfect** option is selected by default.
  - **Scan local removable disk drives:** **[Default]** You should select this check box if you need to scan all the local removable drives attached to the computer.

- **Scan local disk drives:** [Default] You should select this check box if you need to scan all the local drives installed to the computer.
- **Scan network drives:** [Default] You should select this check box if you need to scan all the network drives, including mapped folders and drives, connected to the computer.
- **Scan files of following types:** You should select this option if you need to scan all files, only infectable files, and files by mask. eScan provides you with a list of default files and file types that it scans by mask. You can add more items to this list or remove items as per your requirements by using the **Add / Delete** option.
- **Exclude by mask:** [Default] You should select this check box if you need the File Anti-Virus monitor to exclude all the objects in the Exclude by mask list during real-time monitoring or scanning. You can add or delete a file or a particular file extension by double-clicking the **Add / Delete** option.
- **Not a virus list:** [Default] File Anti-Virus is capable of detecting riskware. Riskware refers to software that are originally not intended to be malicious but somehow can pose as a security risk to critical operating system functions. You can add the names of riskware, such as remote admin software, to the riskware list in the **Not a virus list** dialog box by double-clicking the **Add / Delete** option if you are certain that they are not malicious. The riskware list is empty by default.
- **Exclude folders:** [Default] You should select this option if you need File Anti-Virus to exclude all the listed folders and sub-folders while it is monitoring or scanning folders. You can add or delete folders from the existing list of folders by clicking the **Add / Delete** option.
- **Scan compound objects:** [Default] You should select this check box if you need eScan to scan archives and packed files during scan operations.
- **Enable code analyzer:** You should select this check box if you need eScan to scan your computer for suspicious objects or unknown infections by using the heuristic analyzer. When this check box is selected, File Anti-Virus not only scans and detects infected objects by using the definitions or updates, but it also checks for suspicious files stored on your computer.

2. Options

This tab helps you configure the basic settings for the File Anti-Virus module, such as the maximum size of log files and the path of the destination folder for storing log files, quarantined objects, and report files.



The Options tab

This tab allows you to configure the following settings.

- **Save report file:** You should select this check box if you need eScan to save the reports generated by the File Anti-Virus module. The report file logs information about the scanned files and the action taken by File Anti-Virus when an infected file was found during the scan.

- **Show pack info in the report:** You should select this check box if you need File Anti-Virus to add information regarding scanned compressed files, such as .ZIP and .RAR files to the Monvir.log file.
- **Show clean object info in the report:** You should select this check box if you need File Anti-Virus to add information regarding uninfected files found during a scan operation to the Monvir.log file. You can select this option to find out which files are not infected.
- **Limit size to (Kb):** You should select this check box if you need File Anti-Virus to limit the size of the Monvir.log file. You can double-click the size box and specify the size of the log file.

- **For quarantining of infected objects:** This option helps you specify the destination for storing quarantined objects. By default, the quarantined objects are stored in the C:\Program Files\eScan\Infected folder. You can change the location of the destination folder if required.
- **Enable Auto backup / Restore:** This option helps you back up the critical files of the Windows® operating system installed on your computer and then **automatically** restore the clean files when eScan finds an infection in any of the system files that cannot be disinfected. The following are some of the settings that you can use with this option.

  - **For backup of clean objects:** You can back up uninfected objects and store them in a given folder. By default, these objects are stored in the \FBackup folder. You can change the destination of the backed up objects if necessary.
  - **Do not backup files above size (KB):** This option helps you prevent File Anti-Virus from creating backups of files that are larger than the file size that you have specified.
  - **Minimum disk space (MB):** This option helps you allot the disk space for storing log files.

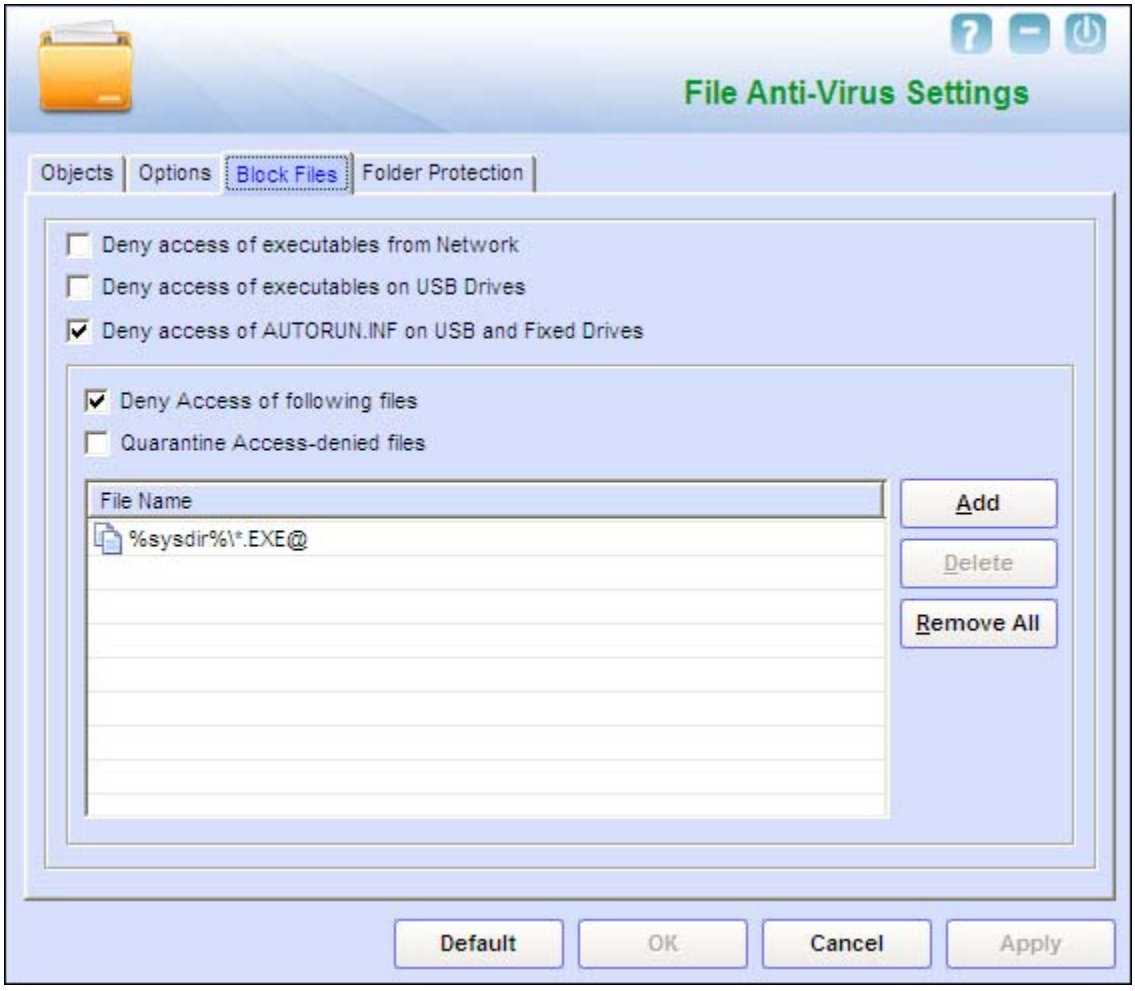
- **Limit file size to (KB):** This option enables you to set a limit size for the objects or files to be scanned. The default value is set to **1024** Kb.
- **Enable Proactive Scan:** When you select this option, File Anti-Virus monitors your computer for suspicious applications and prompts you to block such applications when they try to execute.
- **Use sound effects for the following events:** This option helps you configure eScan to play a sound file and show you the details regarding

the infection within a message box when any malicious software is detected by File Anti-Virus. However, while you need to ensure that the computer's speakers are switched on.

- **Display attention messages:** When this option is enabled, eScan displays an alert, which displays the path and name of the infected object and the action taken by the File Anti-Virus module.

3. Block Files

This tab helps you configure settings for preventing executables and files, such as autorun.inf, on network drives, USB drives, and fixed drives from accessing your computer.



The Block Files tab

This tab allows you to configure the following settings.

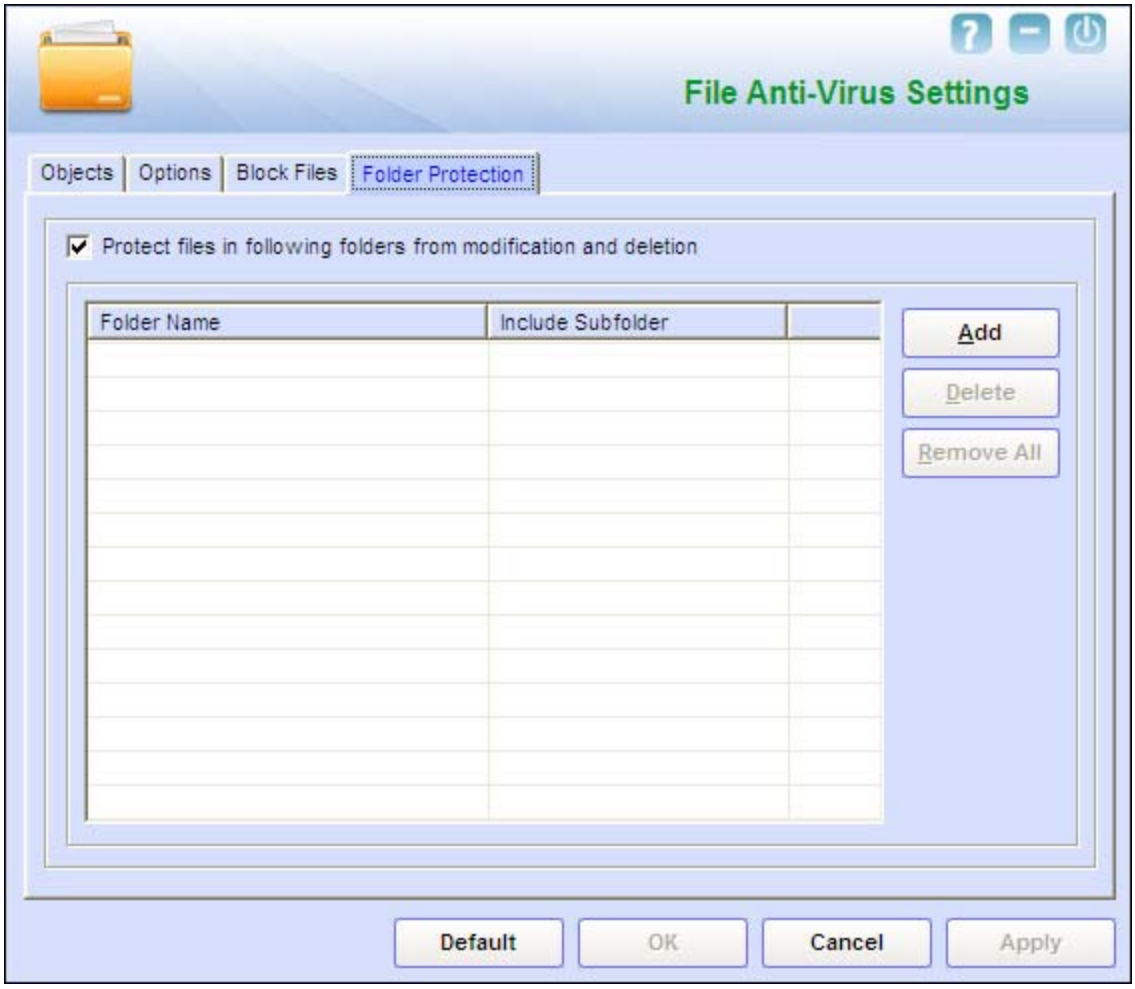
- **Deny access of executables from Network:** You should select this check box if you need to prevent executables on your computer from being accessed from the network.
- **Deny access of executables on USB Drives:** You should select this check box if you need to prevent executables stored on USB drives from being accessed.
- **Deny access of AUTORUN.INF on USB and Fixed Drives:** You should select this check box if you need to prevent executables from USB and fixed drives from being accessed.
- **Deny Access of following files:** You should select this check box if you need to prevent the files in the list from running on your computer.
- **Quarantine Access-denied files:** You should select this check box if you need to quarantine files that have been Access-denied.

You can prevent specific files from running on your computer by adding them to the Block Files list. By default, this list contains the value %sysdir%*.EXE@.

4. Folder Protection

This tab helps you protect specific folders from being modified or deleted by adding them to the Folder Protection list. It allows you to configure the following setting.

- **Protect files in following folders from modification and deletion:** **[Default]** This option is selected by default. You should select this check box if you need the File Anti-Virus module to protect files in specific folders from being modified or deleted.



The Folder Protection tab

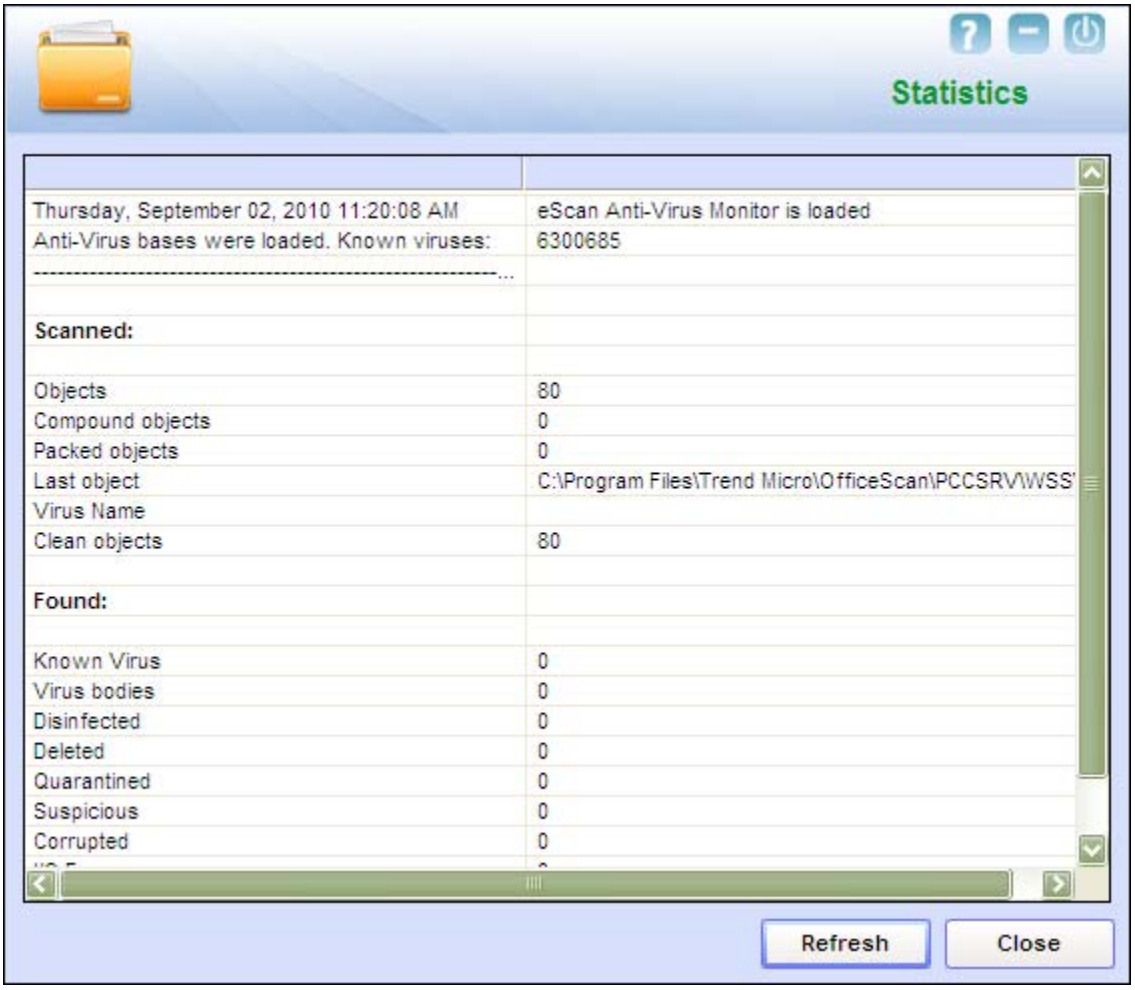
❑ Reports

This section displays the following information.

- **Total Files Scanned:** It shows the total number of files scanned by the real-time File Anti-Virus monitor.
- **Dangerous Objects Detected:** It shows the total number of viruses or malicious software detected by the File Anti-Virus monitor on a real-time basis.
- **Last File Scanned:** It shows the name of the last file scanned by the File Anti-Virus monitor on real-time basis.

In addition, you can view the following reports.

- **View Statistics:** This button displays the latest activity report of the real-time monitor. The report contains information about the number of scanned objects, number of clean objects, and last scanned object.



The Statistics Window

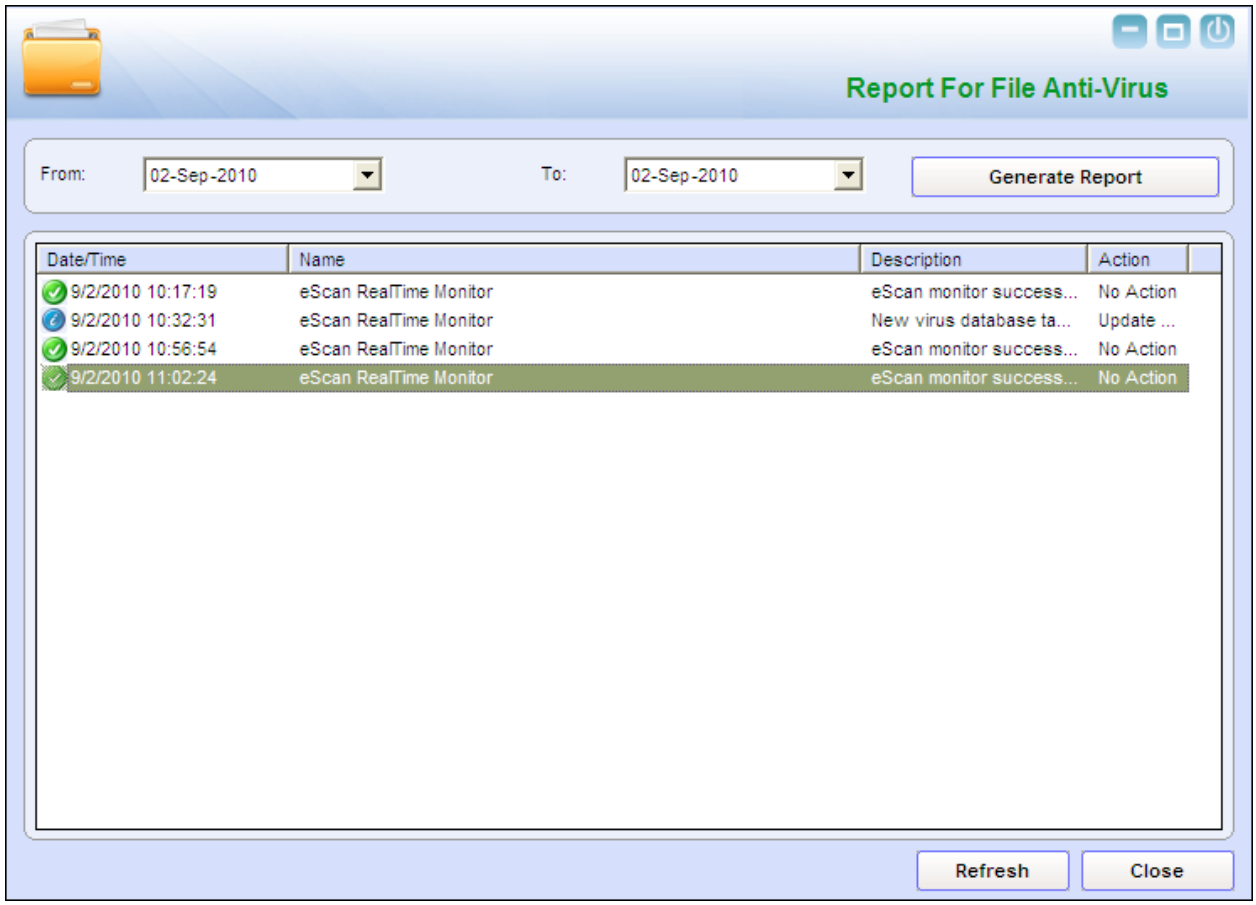
In addition, it displays the following information.

- The current details of the system date, time, and whether the eScan Anti-Virus monitor is running or not.
- The number of viruses detected.
- The results of the most recent scan, such as the last object scanned and the name of the virus detected.

- **View Quarantined Objects:** This button opens the **Quarantine** dialog box, which displays the quarantined files and backup files. This dialog box has the following tabs:

  - **Quarantine:** This tab displays the files that have quarantined. You can restore or delete the quarantined objects by right clicking the object and then clicking the appropriate option.
  - **Backup:** This tab displays the files that were backed up by File Anti-Virus before it tried to disinfect them. You can restore or delete the objects that were backed up by right clicking the object and then clicking the appropriate option. Before clicking any of these buttons, you should ensure that you have selected the appropriate the row in the table for which you need to perform the action.

- **View Report:** This button opens the **Report for File Anti-Virus** window. This window displays the report for the File Anti-Virus module for a given range of dates in a tabular format when you click the **Generate Report** button.



Report for File Anti-Virus

Mail Anti-Virus

Mail Anti-Virus is a part of the Protection feature of eScan. This module scans all incoming and outgoing e-mails for viruses, spyware, adware, and other malicious objects. It also helps you send virus warnings to client computers and allows you to view archived e-mails and reports on the Mail Anti-Virus activities. By default, Mail Anti-Virus scans only the incoming e-mails and attachments but you can configure it to scan outgoing e-mails and attachments as well. Moreover, it helps you notify the sender or system administrator whenever you receive an infected e-mail or attachment.

In addition, Mail Anti-Virus lets you archive e-mails and e-mail attachments so that you can restore them from the backup in case you lose your important e-mails. You can also configure it to compress large e-mail attachments automatically to conserve bandwidth.

Mail Anti-Virus

This module is disabled by default. When you click the Mail Anti-Virus icon in the docking view of the eScan Protection Center, the tabbed page for the module is displayed. This page shows you the options for configuring the module and helps you view reports on the recent scans performed by eScan. The details regarding each of the sections in the right pane are as follows:

❑ Configuration

This section provides you with information regarding the status of Mail Anti-Virus and the action that it will take when it detects a malicious object.

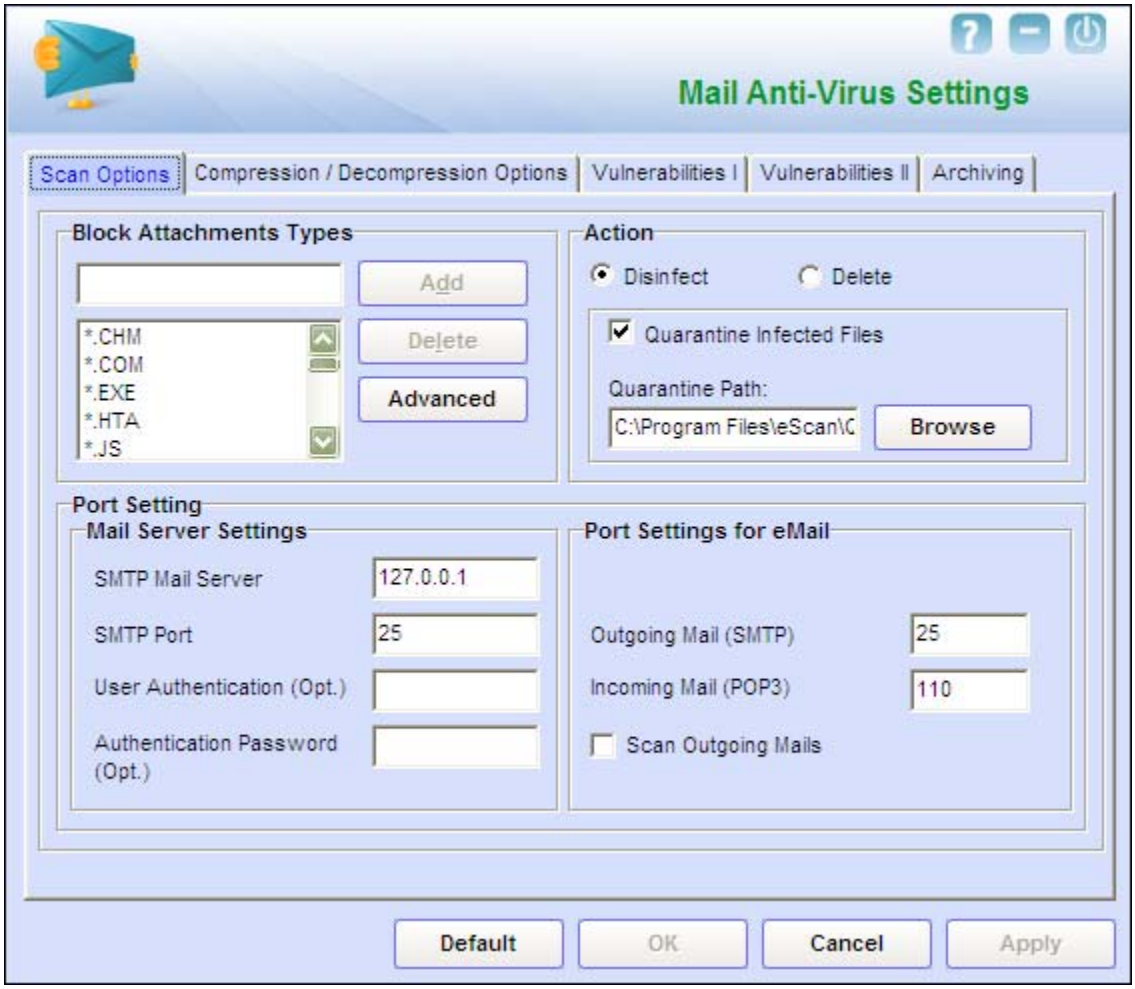
- **Mail Anti-Virus Status:** It shows whether the Mail Anti-Virus module is running or not.
- **Action:** It shows the action that eScan will perform when it detects a malicious object.

In addition, you can configure the following settings.

- **Start/Stop:** This is a toggle button. You can click this button to switch the Mail Anti-Virus module easily from the Start state to the Stop state and vice versa.
- **Settings:** You can click this button to opens the **Mail Anti-Virus Settings** dialog box. This dialog box helps you configure Mail Anti-Virus for real-time monitoring. This dialog box contains several tabs that allow you to configure settings for scanning e-mails; compressing and decompressing attachments; addressing security vulnerabilities, and archiving e-mails.

1. Scan Options

This tab allows you to select the e-mails to be scanned and action that should be performed when a security threat is encountered during a scan operation.

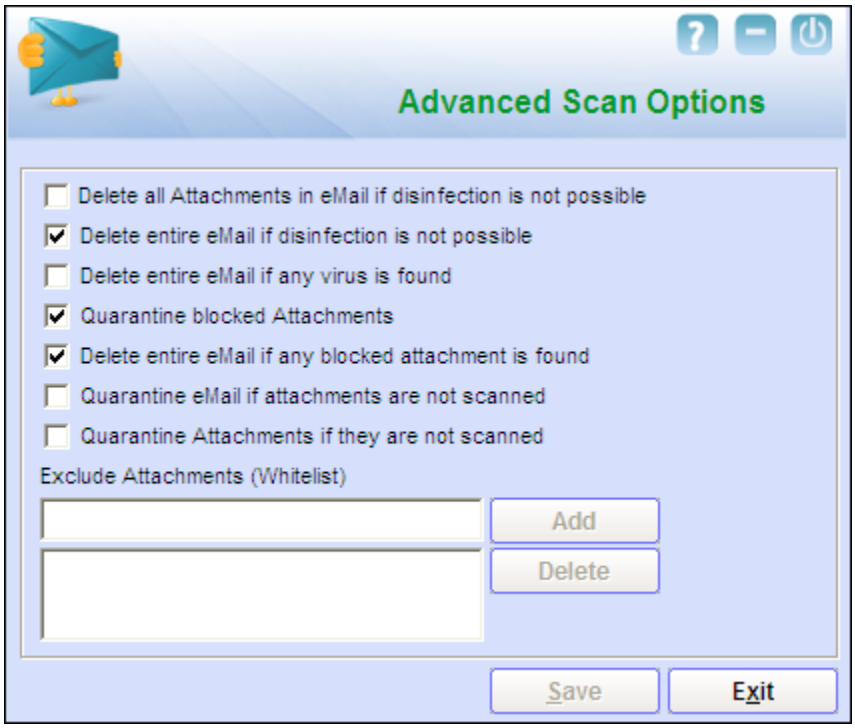


The Scan Options Settings

The **Scan Options** tab helps you configure the following settings.

- **Block Attachments Types:** This section provides you with a predefined list of file types that are often used by virus writers to embed viruses. Any e-mail attachment having an extension included in this list will be blocked or deleted by eScan at the gateway level. You can add file extensions to this list as per your requirements. As a best practice, you should avoid deleting the file extensions that are present in the **Block Attachments Types** list by default. You can also configure advanced settings required to scan e-mails for malicious code.

- **Delete all Attachment in eMail if disinfection is not possible:** You should select this check box if you need to delete all the e-mail attachments that cannot be cleaned.
- **Delete entire eMail if disinfection is not possible:** [Default] You should select this check box if you need to delete the entire e-mail if any attachment cannot be cleaned.
- **Delete entire eMail if any virus is found:** You should select this check box if you need to delete the entire e-mail if any virus is found in the email or the attachmenit is infected.


Advanced Scan Options
Delete all Attachments in eMail if disinfection is not possible
Delete entire eMail if disinfection is not possible
Delete entire eMail if any virus is found
Quarantine blocked Attachments
Delete entire eMail if any blocked attachment is found
Quarantine eMail if attachments are not scanned
Quarantine Attachments if they are not scanned
Exclude Attachments (Whitelist)
Add
Delete
Save
Exit

The Advanced Scan Options Settings

- **Quarantine blocked Attachments:** [Default] You should select this check box if you need to quarantine the attachment if it is has an extension that is blocked by eScan.
- **Delete entire eMail if any blocked attachment is found:** [Default] You should select this check box if you need to delete an e-mail if it contains an attachment with an extension type that is blocked by eScan.
- **Quarantine eMail if attachments are not scanned:** You should select this check box if you need to quarantine an entire e-mail if it contains an attachment that is not scanned by Mail Anti-Virus.

- **Quarantine Attachments if they are not scanned:** You should select this check box if you need to quarantine attachments that are not scanned by Mail Anti-Virus.
- **Exclude Attachments (White List):** This list is empty by default. You can add file names and file extensions that should not be blocked by eScan. You can also configure eScan to allow specific files even though if the file type is blocked. For example, if you have listed *.PIF in the list of blocked attachments and you need to allow an attachment with the name ABCD.PIF, you can add abcd.pif to the Exclude Attachments list. Adding *.PIF files in this section will allow all *.PIF to be delivered. MicroWorld recommends you to add the entire file name like ABCD.PIF.

- **Action:** This section helps you configure the actions to be performed on infected e-mails. These operations are follows:

  - **Disinfect:** **[Default]** This option is selected by default. You should select this option if you need Mail Anti-Virus to disinfect infected e-mails or attachments.
  - **Delete:** You should select this option causes if you need Mail Anti-Virus to delete infected e-mails or attachments.
  - **Quarantine Infected Files:** **[Default]** This check box is selected by default. You should select this check box if you need Mail Anti-Virus to quarantine infected e-mails or attachments. The default path for storing quarantined e-mails or attachments is C:\Program Files\eScan\QUARANT. However, you can specify a different path for storing quarantined files, if required.

- **Port Settings:** You need to specify which ports on the SMTP Mail Server should be used for incoming and outgoing e-mails so that eScan can scan the e-mails sent or received via those ports. This setting also helps you create outbreak alerts, and create warning messages and notifications that eScan should send when it detects any security breach. If you configure Mail Server settings, eScan will send e-mail notifications about the actions that it should perform when it detects infected e-mails. The mail server settings that you need to configure are as follows:

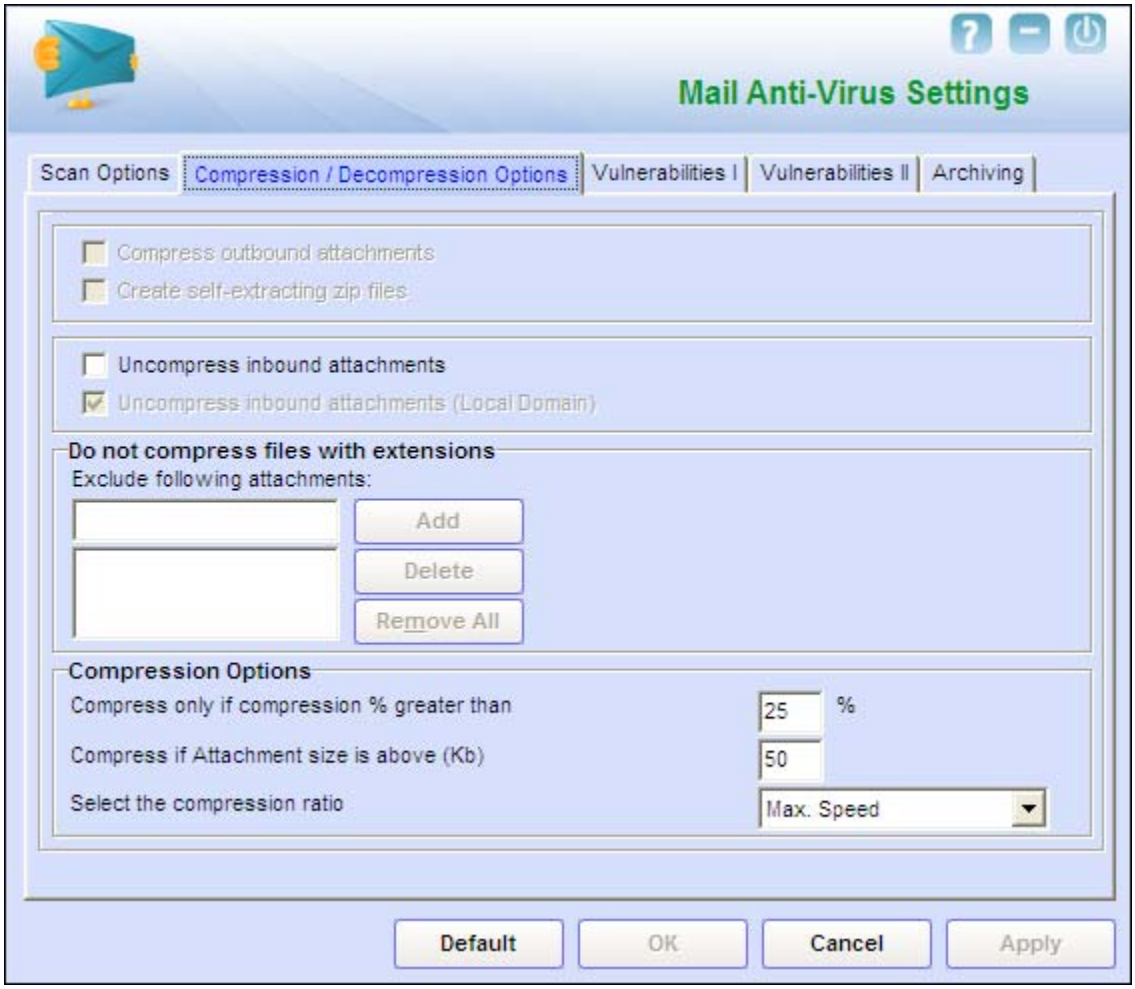
- **SMTP Mail Server:** [Default: 127.0.0.1] You need to specify the IP address of the SMTP Mail Server of your organization or Internet Service Provider (ISP).
- **SMTP Port:** [Default: 25] You need to specify a port number for the SMTP Mail Server of your organization or ISP.
- **User Authentication (Opt.):** You need to provide the user name if the mail server of your organization or ISP requires authentication to send e-mails.
- **Authentication Password (Opt.):** You need to provide the password if the mail server of your organization or ISP requires authentication to send e-mails.

- **Port Settings for eMail:** You can also specify the ports for incoming and outgoing e-mails so that eScan can scan the e-mails sent or received via those ports.

  - **Outgoing Mail (SMTP):** [Default: 25] You need to specify a port number for SMTP.
  - **Incoming Mail (POP3):** [Default: 110] You need to specify a port number for POP3.
  - **Scan Outgoing Mails:** You should select this check box if you need to Mail Anti-Virus to scan outgoing e-mails.

2. Compression / Decompression Options

You can configure the following settings to ensure that the available bandwidth is effectively utilized.



The Compression/Decompression Options Settings

This tab helps you configure the following settings.

- **Compress outbound attachments:** This check box is disabled by default. eScan reduces the size of all outgoing e-mail attachments by compressing them when this check box is enabled.
- **Create self-extracting zip files:** This check box is disabled by default. eScan automatically creates a self-extracting .ZIP file containing the attachment when this check box is enabled. The receiver can click this file to uncompress it. The advantage of this feature is that it eliminates the need for an unzipping tool to be installed on the user's computer. As a best practice, you should select this check box to ensure that the receiver

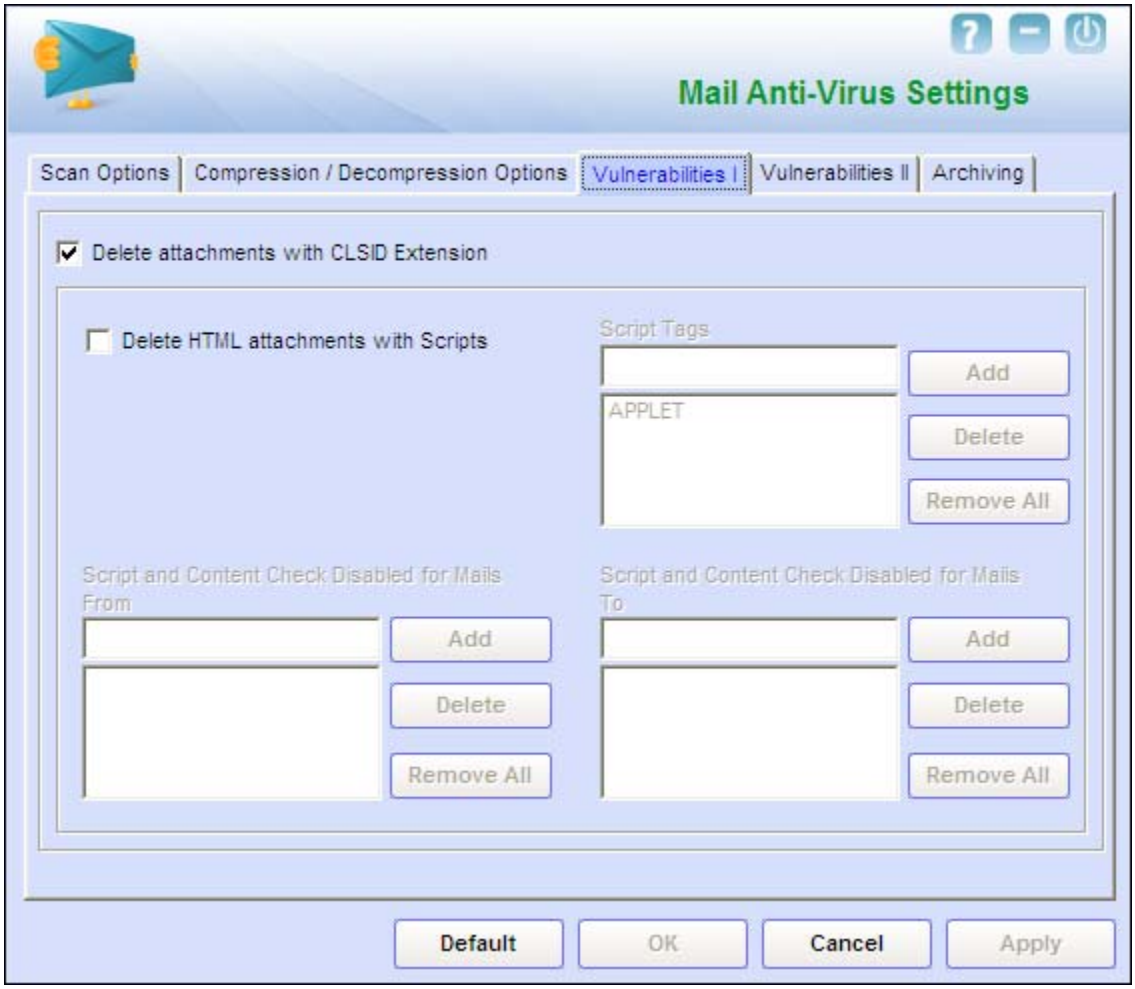
can uncompress the attachment even when a decompression tool is not available.

- **Uncompress inbound attachments:** You should select this check box when you need eScan to automatically unpack compressed files in inbound attachments, scan them, and then deliver them to you.
- **Uncompress inbound attachments (Local Domain):** This check box is disabled by default. When you enable this check box, it appears as selected. You should select this check box when you need eScan to automatically unpack compressed files in inbound attachments, scan them, and then deliver them to the recipients in the local domain.
- **Do not compress files with extensions:** You can exclude specific file types within outgoing e-mail attachments from being compressed by adding them to an excluded attachments list. For example: Excluding files that are already compressed, such as .ZIP files.
- **Compress Options:** This section contains options that help you configure the various parameters for compressing files. These parameters include the percentage up to which the file should be compressed, the minimum size of the files to be compressed, and the compression ratio. This section contains the following options.

    - **Compress only if compression % greater than:** **[Default: 25]** You use this setting to compress all e-mail attachments up to 25 percent or more.
    - **Compress if Attachment size is above (Kb):** **[Default: 50]** You use this setting to compress all e-mail attachments that are larger than the specified size.
    - **Select the compression ratio:** **[Default: Max. Speed]** You can use this setting to specify the compression ratio and make optimum use of system resources. You can configure Mail Anti-Virus to compress files faster or up to the maximum possible compression level.

3. *Vulnerabilities I*

Authors of malicious software often exploit vulnerabilities in Web browsers, such as Internet Explorer® (IE) and propagate malicious software to computers via e-mail clients such as Microsoft® Office Outlook® and Microsoft® Outlook® Express. eScan also includes proactive scanning features that protect your data from such vulnerabilities.



The Vulnerabilities I Settings

The following configuration options are available on this screen.

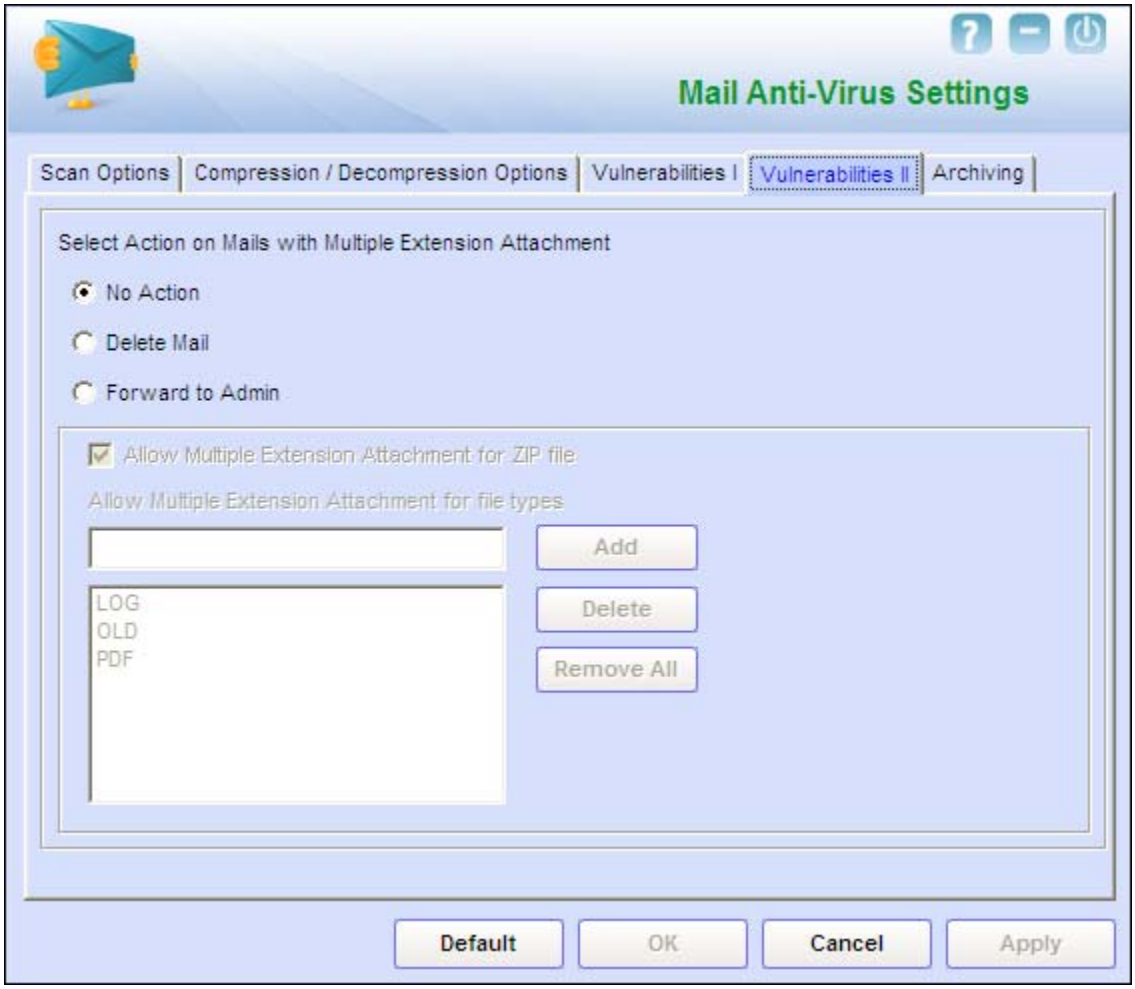
- **Delete attachments with CLSID Extensions:** **[Default]** This option is selected by default. CLSID are hidden files that do not show the actual file extension. If you select this option, Mail Anti-Virus deletes the attachments with CLSID file extensions to prevent dangerous files from exploiting the vulnerabilities in Internet Explorer®.
- **Delete HTML attachments with Scripts:** E-mail clients help you send and receive in different formats, for example, the HTML format. HTML files can include scripts, which are similar to batch files or BAT files. These scripts are embedded within specialized tags and can be used to run malicious code. Hackers often use scripts to execute malicious code on the

computers of their victims. You can configure Mail Anti-Virus to delete HTML attachments with scripts by selecting the **Delete HTML attachments with Script** option. You can also specify the tags that eScan should check for in the attachments so that the attachments containing those tags are deleted. By default, the **Script Tags** list, the **Script and Content Check Disabled for Mails From** list, and the **Script and Content Check Disabled for Mails To** list are disabled.

- **Script Tags:** This section contains a list that contains script tags. eScan will delete all e-mail attachments in the HTML format containing the tags included in this list. You can configure this list to block HTML attachments that contain these tags.
- **Script and Content check disabled for mails From:** This section contains a list of e-mail addresses or domain names that you consider as legitimate senders. This feature of eScan is useful when you need to add a genuine user and receive legitimate e-mails in the HTML format with scripts. You can add e-mail addresses or domain names of such users to the list. All e-mails in the HTML format with scripts coming from those users or domains are automatically delivered to your inbox.
- **Script and Content check disabled for mails To:** This section contains a list of e-mail addresses or domain names, which you consider as legitimate recipients. This feature of eScan is useful when you need to send e-mails in the HTML format with scripts to a legitimate user. You can add e-mail addresses or domain names of such users to this list.

4. Vulnerabilities II

eScan helps you choose the action that you can take on mails containing attachments with multiple extensions.



The Vulnerabilities I Settings

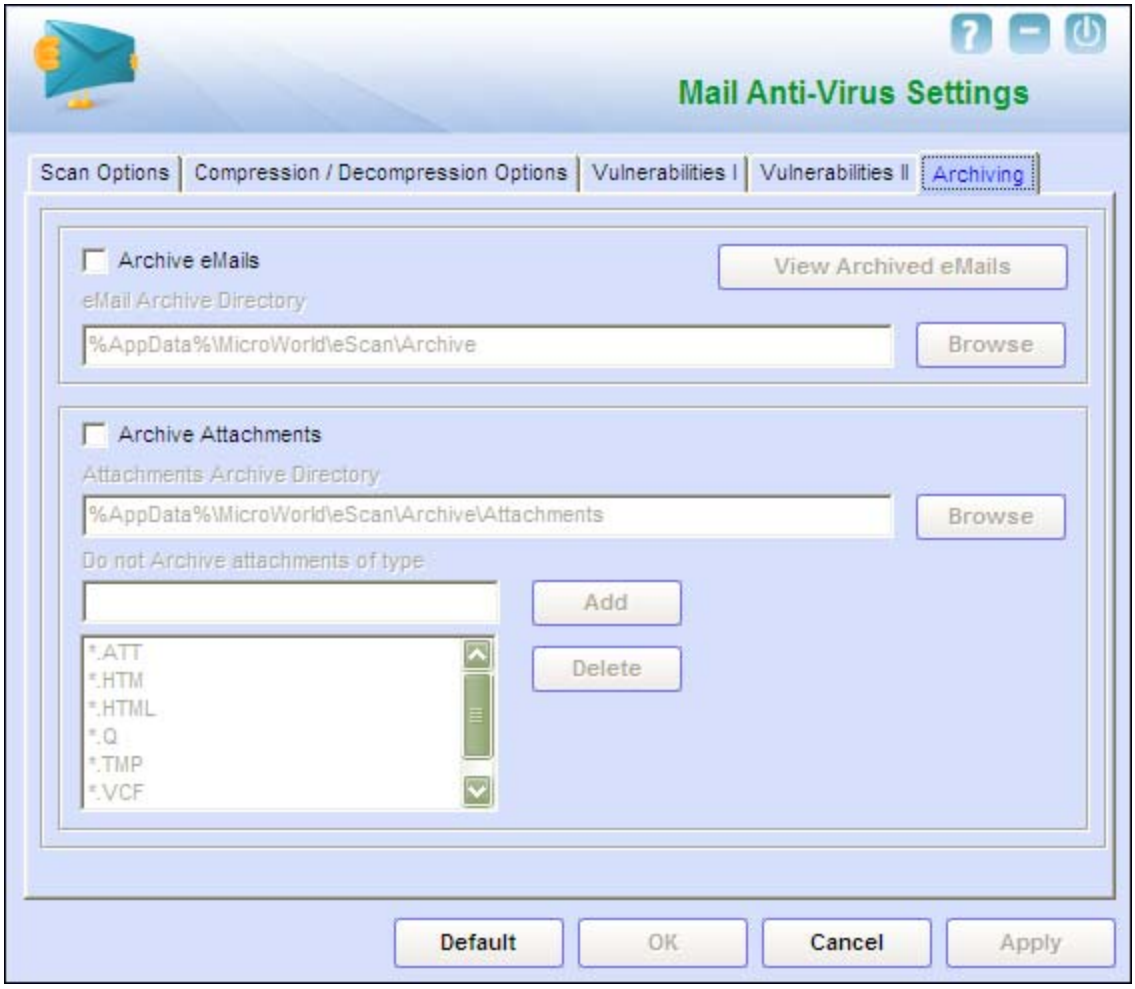
This tab helps you configure the following settings.

- **Select Action on Mails with Multiple Extension Attachment:** You can configure Mail Anti-Virus to perform specific actions if attachments contain files with multiple extensions. You can configure Mail Anti-Virus to refrain from taking any action on the e-mail, delete it, or forward it to the administrator. The settings under **Allow Multiple Extension attachment for ZIP file** are disabled by default. They are enabled only when you select the **Delete Mail** option or the **Forward to Admin** option.
- **Allow Multiple Extension attachment for ZIP file:** You should select this check box if you need Mail Anti-Virus to allow compressed files with multiple extensions as e-mail attachments.

- **Allow Multiple Extension Attachment for file types:** You can add file extensions to allow such attachments containing multiple extensions to be delivered to the user's inbox.

5. Archiving

This screen helps you configure settings for archiving e-mails and e-mail attachments.



The Archiving Settings

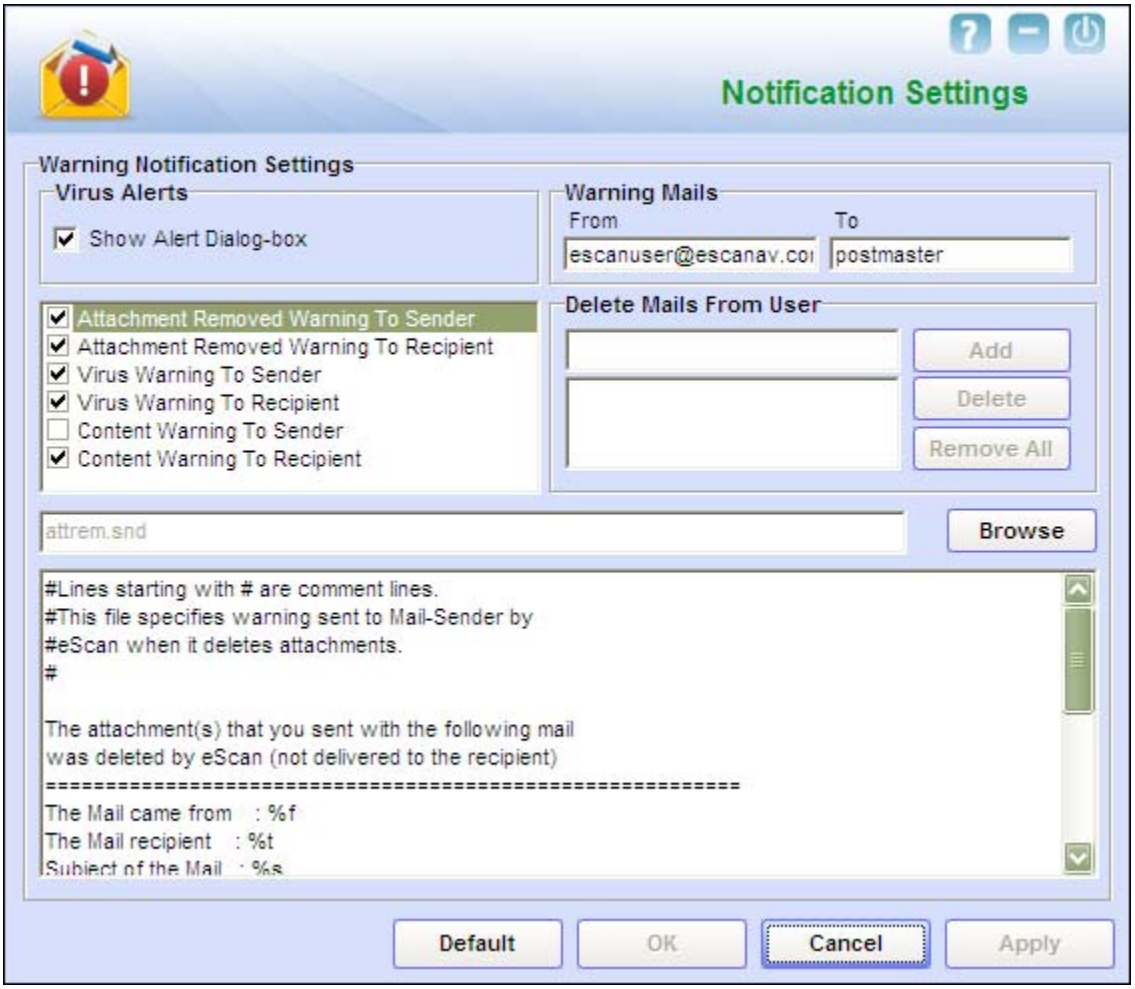
The following configuration options are available on this screen.

- **Archive eMails:** This option helps you archive or back up all e-mails that you have sent or received. Mail Anti-Virus provides you with the facility of backing up your e-mails to a given folder. The default path for storing archived e-mails is %UserProfile%\Application

Data\MicroWorld\eScan\Archive. The **eMail Archive Directory** box is disabled by default. Therefore, to specify the path of the backup folder, you need to select the **Archive eMails** check box.

- **Archive Attachments:** You should select this check box if you need to archive or back up all sent or received e-mail attachments to a given folder. However, to specify the path of the backup folder, you need to select the **Archive Attachments** check box because the **Attachments Archive Directory** box is disabled by default. The default path for storing archived e-mail attachments is %UserProfile%\Application Data\MicroWorld\eScan\Archive\Attachments. At times, you may not require e-mail attachments of a specific file type. In that case, you can excluded certain file types, such as *.VCF, *.HTM, and *.HTML, from being archived by adding them to the **Do not Archive attachments of type** list.

- **Notification:** You can click this button to open the **Notification Settings** dialog box, which helps you configure the notification settings for the Mail Anti-Virus module. By configuring this module, you can send e-mails to specific recipients when malicious code is detected in an e-mail or e-mail attachment. This dialog box helps you configure the notification settings for sending alerts and warning messages to the senders or recipients of an infected message.



The Notification Settings

You can configure the following notification settings.

- **Virus Alerts:** [Default] You should select this check box if you need Mail Anti-Virus to alert you when it detects a malicious object in an e-mail.
- **Warning Mails:** You configure this setting if you need Mail Anti-Virus to send warning e-mails and alerts to a given sender or recipient. The default sender is **escanuser@escanav.com** and the default recipient is **postmaster**.
- **Attachment Removed Warning To Sender:** [Default] You should select this check box if you need Mail Anti-Virus to send a warning message to the sender of an infected attachment. Mail Anti-Virus sends this e-mail when it encounters a virus-infected attachment in an e-mail. The content of the e-mail that is sent is displayed in the preview box.

- **Attachment Removed Warning To Recipient:** [Default] You should select this check box if you need Mail Anti-Virus to send a warning message to the recipient when it removes an infected attachment. The content of the e-mail that is sent is displayed in the preview box.
- **Virus Warning To Sender:** [Default] You should select this check box if you need Mail Anti-Virus to send a virus-warning message to the sender. The content of the e-mail that is sent is displayed in the preview box.
- **Virus Warning To Recipient:** [Default] You should select this check box if you need Mail Anti-Virus to send a virus-warning message to the recipient. The content of the e-mail that is sent is displayed in the preview box.
- **Content Warning To Sender:** You should select this check box if you need Mail Anti-Virus to send a content warning message to the sender. The content of the e-mail that is sent is displayed in the preview box.
- **Content Warning To Recipient:** [Default] You should select this check box if you need Mail Anti-Virus to send a content warning message to the recipient. The content of the e-mail that is sent is displayed in the preview box.
- **Delete Mails From User:** You can configure eScan to automatically delete e-mails that have been sent by specific users. For this, you need to add the e-mail addresses of such users to the Delete Mails From User list. The **Delete Mails From User** section is disabled by default. As you type in some text in the **Delete Mails From User** box and add e-mail addresses, the appropriate user interface elements will be enabled.

❑ Reports

This section displays the following information.

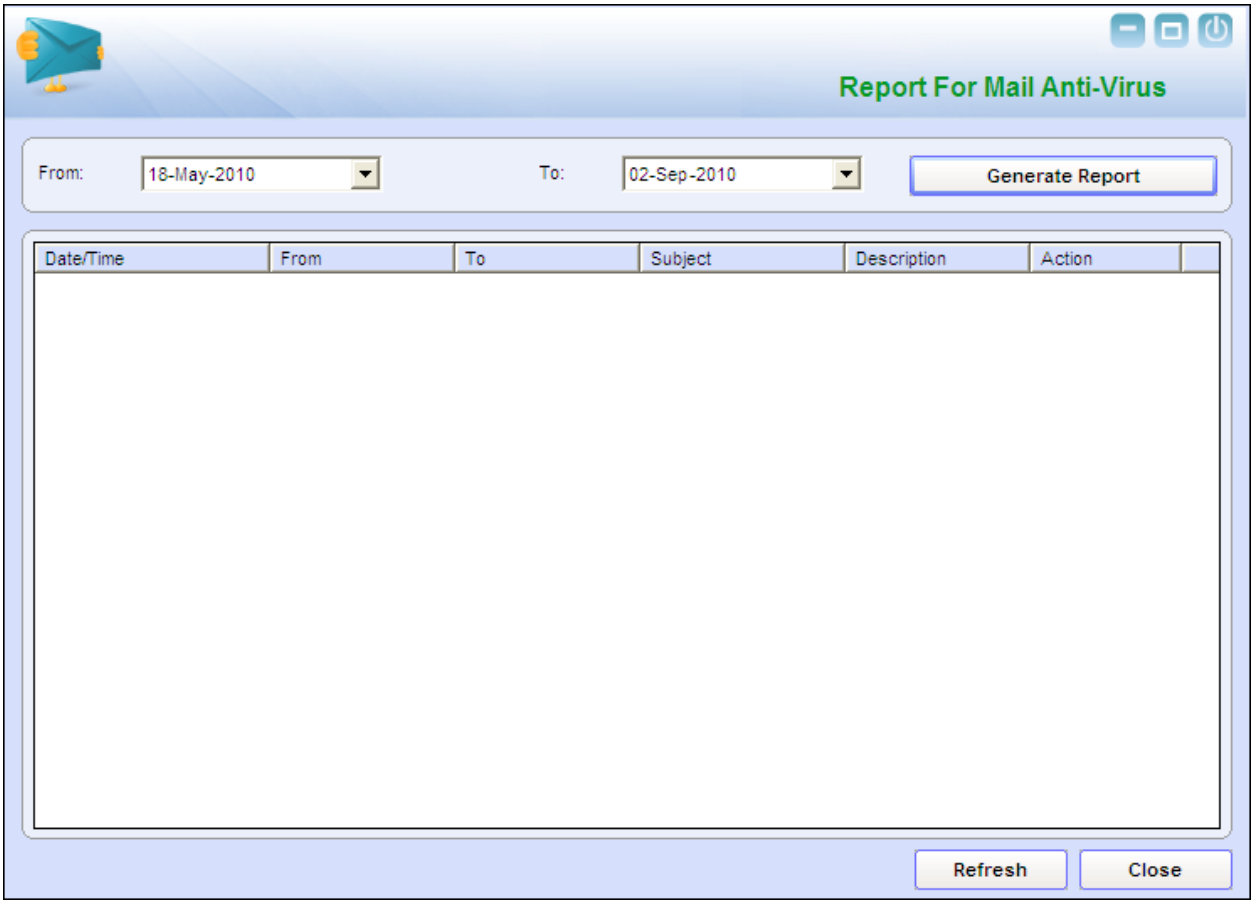
- **Total Mails Scanned:** It shows the total number of e-mails scanned by Mail Anti-Virus on a real-time basis.
- **Total Infected Objects:** It shows the total number of infected objects found by Mail Anti-Virus on a real-time basis.

In addition, you can view the following reports.

- **View Archived Mails:** You can click this button to open the **View Archived eMails** window.

  (See the section on the **View Archived eMails** window under **Archiving**.)

- **View Report:** You can click this button to open the **Report for Mail Anti-Virus** window. This window displays the summary of infected e-mails and the action taken by Mail Anti-Virus on such e-mails for a given range of dates in a tabular format when you click the **Generate Report** button.



Reports for Mail Anti-Virus

Anti-Spam

Anti-Spam is a part of eScan's Protection feature. This module filters all your junk and spam e-mails by using the NILP technology and sends content warnings to specified recipients. It also provides reports about Anti-Spam activities and allows you to view quarantined mails and ham mails.

Anti-Spam

The Anti-Spam icon is disabled by default. When you click this icon in the docking view of eScan Protection Center, the tabbed page for the Anti-Spam module is displayed. This page provides you with the options for configuring the module and helps you view reports on the recent scans performed by eScan. The details regarding each of these sections are as follows:

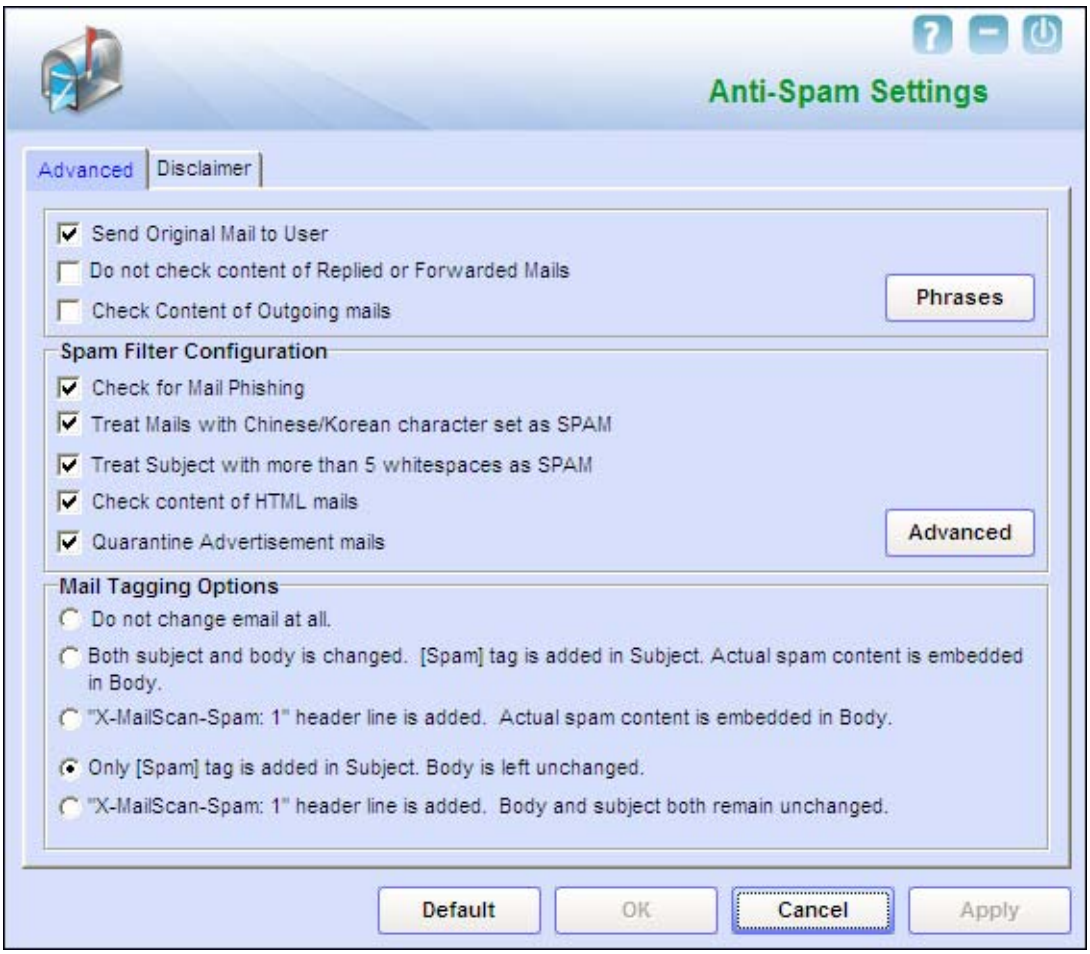
❑ Configuration

This section displays the following information.

- **Anti-Spam Status:** It shows whether the Anti-Spam module is running or not.
- **Mail Phishing Filter:** It shows whether the Mail Phishing Filter is running or not.
- **Action:** It shows the action that eScan will perform if a malicious object is detected.

In addition, you can configure the following settings.

- **Start/Stop:** This button is a toggle button. You can click this button to enable or disable the Anti-Spam module.
- **Settings:** You can click this button to open the **Anti-Spam Settings** dialog box. This dialog box contains options that help you configure Anti-Spam to prevent spam e-mails from reaching your inbox. This dialog box has the following tabs.


Anti-Spam Settings
Advanced
Disclaimer
Send Original Mail to User
Do not check content of Replied or Forwarded Mails
Check Content of Outgoing mails
Phrases
Spam Filter Configuration
Check for Mail Phishing
Treat Mails with Chinese/Korean character set as SPAM
Treat Subject with more than 5 whitespaces as SPAM
Check content of HTML mails
Quarantine Advertisement mails
Advanced
Mail Tagging Options
Do not change email at all.
Both subject and body is changed. [Spam] tag is added in Subject. Actual spam content is embedded in Body.
"X-MailScan-Spam: 1" header line is added. Actual spam content is embedded in Body.
Only [Spam] tag is added in Subject. Body is left unchanged.
"X-MailScan-Spam: 1" header line is added. Body and subject both remain unchanged.
Default
OK
Cancel
Apply

The Advanced Settings

1. Advanced

This tab provides you with options for configuring the general e-mail options, spam filter, and tagging e-mails in Anti-Spam.

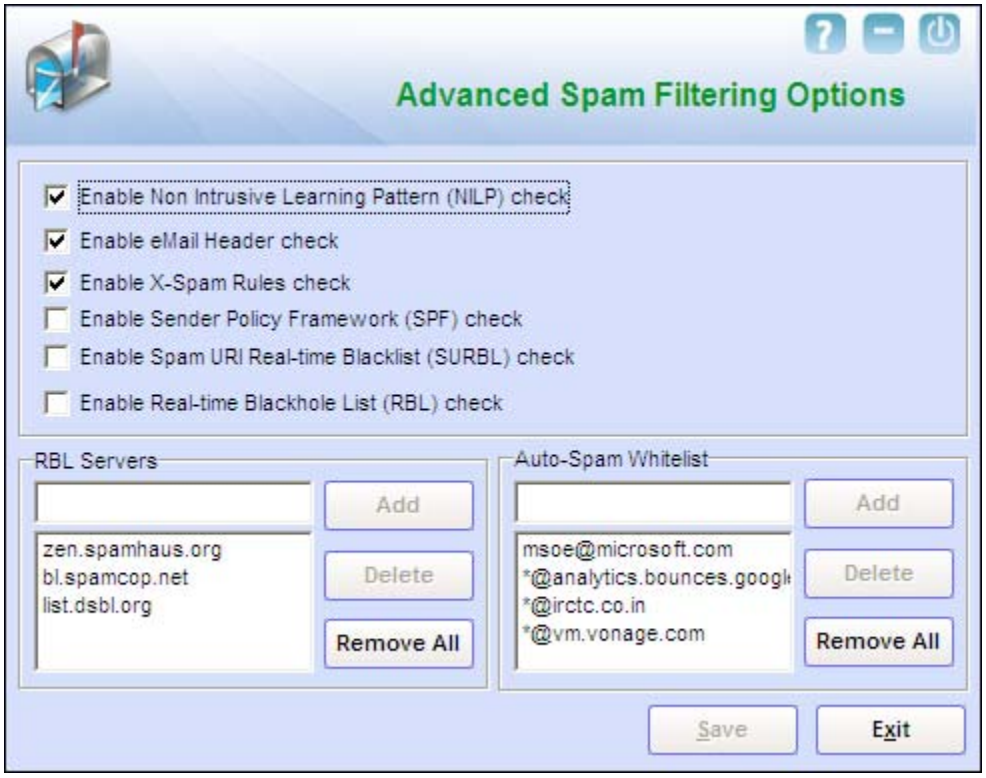
- **General Options:** This section helps you configure the general Anti-Spam settings.

  - **Send Original Mail to User:** **[Default]** This check box is selected by default. eScan creates the Spam folder within the e-mail client. When an e-mail is tagged as SPAM, it is moved to this folder. You should select this check box if you need to send original e-mail that is tagged as spam to the recipient as well.
  - **Do not check content of Replied or Forwarded Mails:** You can select this check box if you need to ensure that eScan does not check the contents of e-mails that you have either replied or forwarded to other recipients.
  - **Check Content of Outgoing mails:** You can select this check box if you need Anti-Spam to check outgoing e-mails for restricted content.
  - **Phrases:** You can click the **Phrases** button to open the **Phrases** dialog box. This dialog box helps you configure additional e-mail-related options. In addition, it allows you to specify a list of words that the user can either allow or block. This list is called the **user specified whitelist**. You can specify certain words or phrases so that mails containing those words or phrases in the subject, header, or body are recognized as spam and are quarantined or deleted. The dialog box uses the following color codes to categorize e-mails.

    - **User specified whitelist of words/phrases:** (Color Code: **GREEN**) You should click this option to list the words or phrases that are present in the whitelist. A phrase that is added to the whitelist cannot be edited, enabled, or disabled.
    - **User specified List of Blocked words/phrases:** (Color Code: **RED**) You should click this option to list the words or phrases that are defined in block list.
    - **User specified words/phrases disabled:** (Color Code: **GRAY**) You should click this option to list the words or phrases that are defined excluded during scans. The options in the **Phrases to Check** dialog box are disabled by default.

- **Spam Filter Configuration:** This section provides you with options for configuring the spam filter. All options in this section are selected by default.

    - **Check for Mail Phishing:** [Default] You should select this check box if you need Anti-Spam to check for fraudulent e-mails and quarantine them.
    - **Treat Mails with Chinese /Korean character set as SPAM:** [Default] When this check box is selected, eScan scans e-mails with Chinese or Korean characters. This check is based on the research data conducted by MicroWorld's various spam e-mail samples collected from around the globe. From these samples, it was observed that spammers often use Chinese or Korean characters in their e-mails.
    - **Treat Subject with more than 5 whitespaces as SPAM:** [Default] In its research, MicroWorld found that spam e-mails usually contain more than five consecutive white spaces. When this check box is selected, Anti-Spam checks the spacing between characters or words in the subject line of e-mails and treats e-mails with more than five whitespaces in their subject lines as spam e-mails.
    - **Check content of HTML mails:** [Default] You should select this check box when you need Anti-Spam to scan e-mails in HTML format along with textual content.
    - **Quarantine Advertisement mails:** [Default] You should select this check box when you need Anti-Spam to check for advertisement types of e-mails and quarantine them.
    - **Advanced:** You can click the **Advanced** button to open the **Advanced Spam Filtering Options** dialog box. This dialog box helps you configure the following advanced options for controlling spam.



The Advanced Spam Filtering Options

- **Enable Non Intrusive Learning Pattern (NILP) check:** [Default] NILP is MicroWorld's revolutionary technology that uses Bayesian Filtering and works on the principles of Artificial Intelligence (AI) to analyze each e-mail and prevents spam and phishing e-mails from reaching your inbox. It has self-learning capabilities and it updates itself by using regular research feeds from MicroWorld servers. It uses an adaptive mechanism to analyze each e-mail and categorize it as spam or ham based on the behavioral pattern of the user. You should select this check box if you need to enable NILP check.
- **Enable eMail Header check:** [Default] You should select this check box if you need to check the validity of certain generic fields like From, To, and CC in an e-mail and marks it as spam if any of the headers are invalid.
- **Enable X-Spam Rules check:** [Default] X-Spam Rules are rules that describe certain characteristics of an e-mail. It checks whether the words in the content of e-mails are present in

eScan's database. This database contains a list of words and phrases, each of which is assigned a score or threshold. The X-Spam Rules Check technology matches X-Spam Rules with the mail header, body, and attachments of each e-mail to generate a score. If the score crosses a threshold value, the mail is considered as spam. Anti-Spam refers to this database to identify e-mails and takes action on them.

- **Enable Sender Policy Framework (SPF) check:** SPF is a world-standard framework that is adopted by eScan to prevent hackers from forging sender addresses. It acts a powerful mechanism for controlling phishing mails. You should select this check box if you need Anti-Spam to check the SPF record of the sender's domain. However, your computer should be connected to the Internet for this option to work.
- **Enable Spam URI Realtime Blacklist (SURBL) check:** You should select this option if you need Anti-Spam to check the URLs in the message body of an e-mail. If the URL is listed in the SURBL site, the e-mail will be blocked from being downloaded. However, your computer should be connected to the Internet for this option to work.
- **Enable Realtime Blackhole List (RBL) check:** You should select this option if you need Anti-Spam to check the sender's IP address in the RBL sites. If the sender IP address is blacklisted in the RBL site, the e-mail will be blocked from being downloaded. However, your computer should be connected to the Internet for this option to work.
- **RBL Servers:** RBL is a DNS server that lists IP addresses of known spam senders. If the IP of the sender is found in any of the blacklisted categories, the connection is terminated. The RBL Servers list contains addresses of servers and sites that maintain information regarding spammers. You can add or change addresses to this list as per your requirements.
- **Auto-Spam Whitelist:** Unlike normal RBLs, SURBL scans e-mails for names or URLs of spam Web sites in the message body. It terminates the connection if the IP of the sender is found in any of the blacklisted categories. This contains a list of valid e-mail addresses that can bypass the above Spam filtering options. It thus allows e-mails from the whitelist to be downloaded to the recipient's inbox.

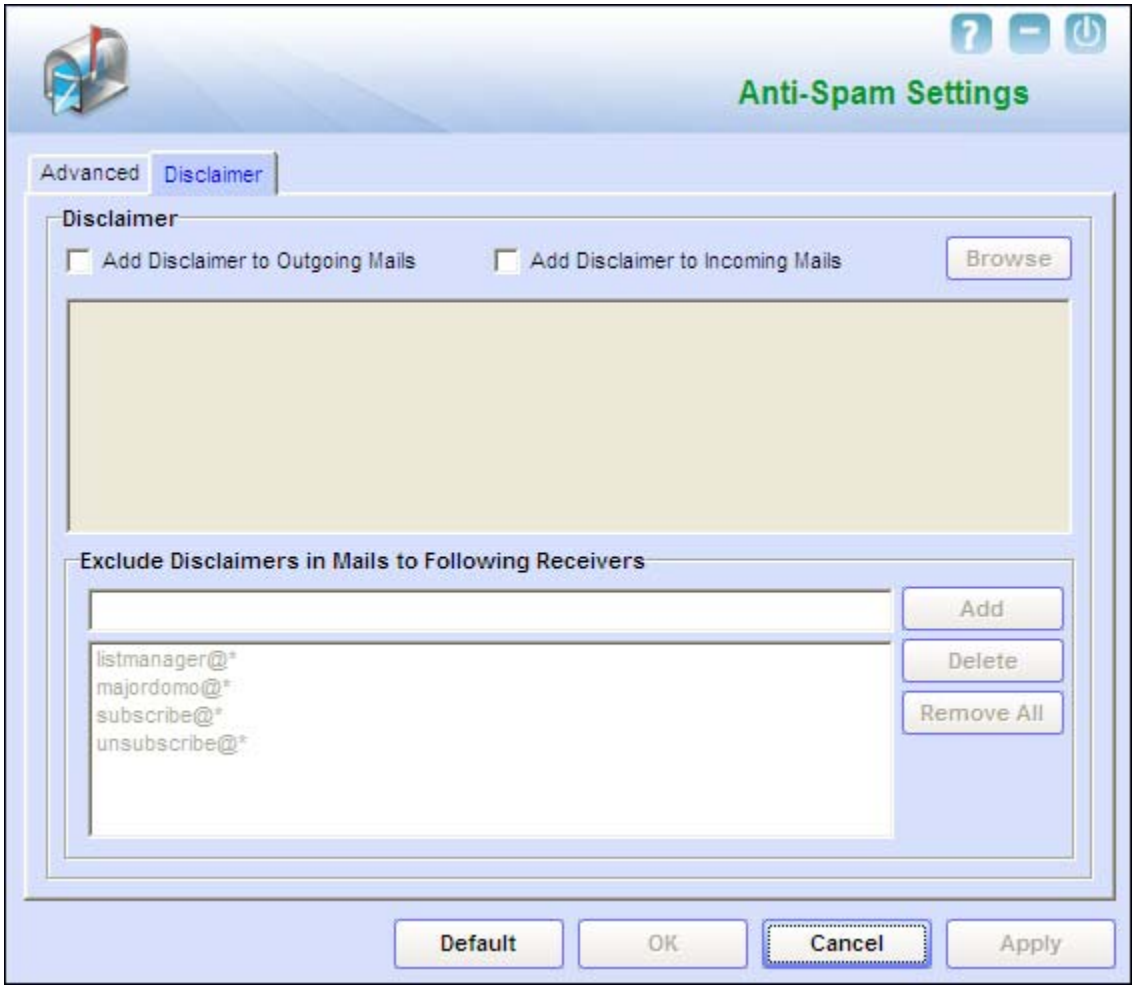
Note: If you have a direct connection to the Internet, the **Enable Spam URI Realtime Blacklist (SURBL) check** and **Enable Realtime Blackhole List (RBL) check** check boxes will be enabled.

- **Mail Tagging Options:** Anti-Spam also includes some mail tagging options, which are described as follows:

  - **Do not change email at all:** You should select this option when you need to prevent Anti-Spam from adding the [Spam] tag to e-mails that have been identified as spam.
  - **Both subject and body is changed: [Spam] tag is added in Subject: Actual spam content is embedded in Body:** This option helps you identify spam e-mails. When you select this option, Anti-Spam adds a [Spam] tag in the subject line and the body of the e-mail that has been identified as spam.
  - **"X-MailScan-Spam: 1" header line is added: Actual spam content is embedded in Body:** This option helps you add a [Spam] tag in the body of the e-mail that has been identified as spam. In addition, it adds a line in the header line of the e-mail.
  - **Only [Spam] tag is added in Subject: Body is left unchanged:** This option helps you add the [Spam] tag only in the subject of the e-mail, which has been identified as spam.
  - **"X-MailScan-Spam: 1" header line is added: Body and subject both remain unchanged:** **[Default]** This option helps you add a header line to the e-mail. However, it does not add any tag to the subject line or body of the e-mail.

2. Disclaimer

The disclaimer is a footer or signature that is appended to all e-mails. The disclaimer can be added in the space provided.



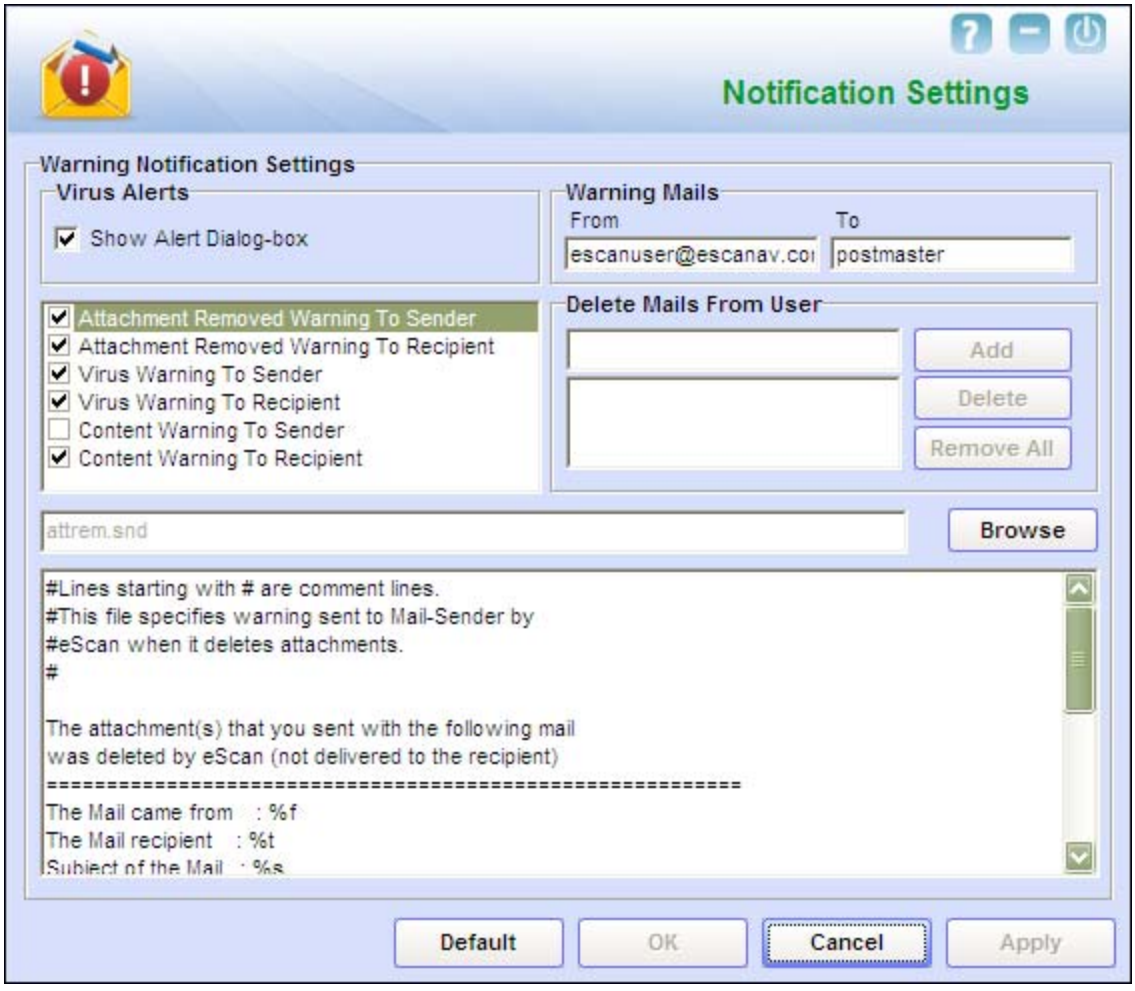
The Disclaimer Settings

The **Disclaimer** tab helps you configure the following settings.

- **Add Disclaimer to Outgoing e-mails:** You should select this check box when you need to add a disclaimer to all outgoing e-mails. This helps to make the recipient aware that the e-mail is scanned and free of viruses.
- **Add Disclaimer to Incoming e-mails:** You should select this check box when you need to add a disclaimer to all incoming e-mails. Thus, you make the recipient aware that the e-mail is scanned and free of viruses. You can add a custom disclaimer by either typing the text of the disclaimer in the **Disclaimer** box or by selecting the file containing the disclaimer text by clicking **Browse**.

- **Outgoing mails excluded from adding Disclaimer:** This section is enabled when the **Add Disclaimer to Outgoing e-mails** check box is selected. By selecting this check box, you can restrict Anti-Spam from appending the disclaimer to specific e-mail addresses or domains by adding them to a list.

- **Notification:** This button opens the **Notification Settings** dialog box. You can configure the notification settings for the Anti-Spam module by using this dialog box. By configuring this module, you can send e-mails to specific recipients when a particular event occurs.



The Notification Settings

The warning notification settings that you can configure on this screen are as follows:

- **Virus Alerts:** You should select this check box if you need Anti-Spam to display an alert box notifying you of a virus infection.
- **Warning Mails:** You should select this check box if you need Anti-Spam to send warning e-mails to a given recipient. The default sender is **escanuser@escanav.com** and the default recipient is postmaster. In addition, you can configure Anti-Spam to send warning e-mails and alerts to senders or recipients. When you click on any one of these options, the corresponding e-mail message is displayed in the preview box.
- **Attachment Removed Warning To Sender:** **[Default]** You should select this check box if you need Anti Spam to send a warning message to the sender of an infected attachment. Anti Spam sends this e-mail when it encounters a virus-infected attachment in an e-mail. The content of the e-mail that is sent is displayed in the preview box.
- **Attachment Removed Warning To Recipient:** **[Default]** You should select this check box if you need Anti Spam to send a warning message to the recipient when it removes an infected attachment. The content of the e-mail that is sent is displayed in the preview box.
- **Virus Warning To Sender:** **[Default]** You should select this check box if you need Anti Spam to send a virus-warning message to the sender. The content of the e-mail that is sent is displayed in the preview box.
- **Virus Warning To Recipient:** **[Default]** You should select this check box if you need Anti Spam to send a virus-warning message to the recipient. The content of the e-mail that is sent is displayed in the preview box.
- **Content Warning To Sender:** You should select this check box if you need Anti Spam to send a content warning message to the sender. The content of the e-mail that is sent is displayed in the preview box.
- **Content Warning To Recipient:** **[Default]** You should select this check box if you need Anti Spam to send a content warning message to the recipient. The content of the e-mail that is sent is displayed in the preview box.
- **Delete Mails From User:** You can set eScan to automatically delete e-mails that have been sent by specific users. For this, you need to add the e-mail addresses of such users to the Delete Mails From User list.

❑ Reports

This section displays the following information.

- **Total Quarantined Mails:** It shows the total number of files scanned by the real-time Anti-Spam monitor.

- **Total Clear Mails:** It shows the total number of viruses or malicious software detected by the Anti-Spam monitor on a real-time basis.

In addition, you can view the following reports.

- **View Quarantined Mails:** This button opens the **View Quarantined Mails** window, which displays the list of quarantined e-mails that have been quarantined by Anti-Spam. With the help of this window, you can configure the following settings. You can specify the path of the folder where you need to store the archived e-mails and can also specify the format for storing e-mails. In addition, you can view the contents of e-mails, add the sender's e-mail id to the white list or add the reserve content of the selected e-mail to the Hide E-Mail List.
- **View Ham Mails:** This button opens the **View Ham Mails** window, which displays the report of all the ham e-mails identified by eScan and have been archived by Mail Anti-Virus. As in the case of quarantined mails, you can specify the path of the folder where you need to store the archived e-mails and can also specify the format for storing e-mails.
- **View Report:** This button displays the **Report for the Anti-Spam** window. This window displays the report for the Anti-Spam module for a given range of dates in a tabular format when you click the **Generate Report** button.

Firewall

Firewall is a security feature of eScan's Protection module. It is designed to monitor all incoming and outgoing network traffic and protect your computer from all types of network-based attacks. eScan includes a set of predefined access control rules that you can remove or customize as per your requirements. These rules enforce a boundary between your computer and the network. Therefore, the Firewall feature first checks the rules, analyzes network packets, and filters them on the basis of the specified rules.

Firewall

Benefits of the Firewall feature

When you connect to the Internet, you expose your computer to various security threats. The Firewall feature of eScan protects your data when you:

- Connect to Internet Relay Chat (IRC) servers and join other people on the numerous channels on the IRC network.

- Use Telnet to connect to a server on the Internet and then execute the commands on the server.
- Use FTP to transfer files from a remote server to your computer.
- Use Network basic input/output system (NetBIOS) to communicate with other users on the LAN that is connected to the Internet.
- Use a computer that is a part of a Virtual Private Network (VPN).
- Use a computer to browse the Internet.
- Use a computer to send or receive e-mail.

By default, the firewall operates in the **Limited Filter** mode. In this mode, it filters only the incoming traffic. However, you can customize the firewall by using options such as **Turn Off** and **Block All** and by changing the mode to **Interactive Filter**. The eScan Firewall also allows you to specify different set of rules for allowing or blocking incoming or outgoing traffic. These rules include zone rules, expert rules, application rules, trusted Media Access Control (MAC) address, and local IP list. You can also view detailed reports regarding the network traffic for your computer in both graphical and text-only formats.

When you select the Firewall icon, the tabbed page of Protection Center provides you with information regarding its status, options for configuring the module, and links to reports on the recent scans performed by the module. This page shows two sections: Configuration and Reports, which are described as follows:

❑ Configuration

This section displays the following information.

- **Firewall Status:** It shows whether the Firewall module is running or not. By default, Firewall runs in the **Allow All** mode.
- **Filteration System:** It shows the filtration system in use by the Firewall module.

In addition, you can configure the following settings.

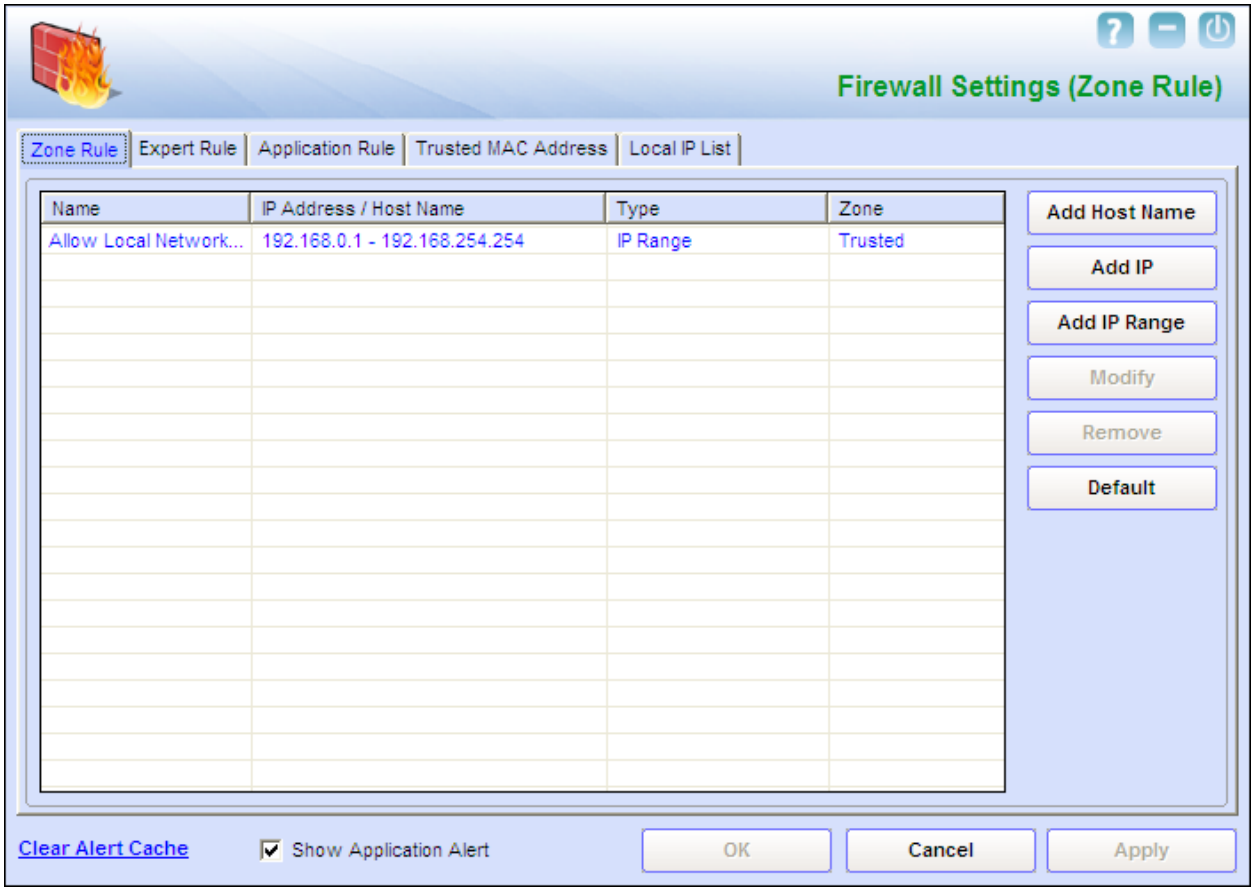
- **Turn Off:** **[Default]** You can click this button to disable the eScan Firewall. When you select this option, eScan stops monitoring all incoming and outgoing network traffic.
- **Limited Filter:** You can click this button to enable the **Limited Filter** mode. When the Firewall module is in this mode, it monitors all incoming traffic and helps you allow or block traffic as per the defined conditions or rules.
- **Interactive Filter:** You can click this button to enable the **Interactive Filter** mode. When the Firewall module is in this mode, it needs user intervention. It monitors all

the incoming and outgoing network traffic and allows or blocks traffic as per the user's choice.

- **Block All:** You can click this button to block all the incoming and outgoing network traffic.
- **Settings:** You can click this button to open the **Firewall Settings** dialog box, which helps you configure the various firewall rules and settings. These tabs are described as follows:

1. Zone Rule

This tab contains settings that help you configure network access rules that specify which IP address, host name, or IP range of computers can access your computer.



The Zone Rule Tab

This tab includes the following buttons.

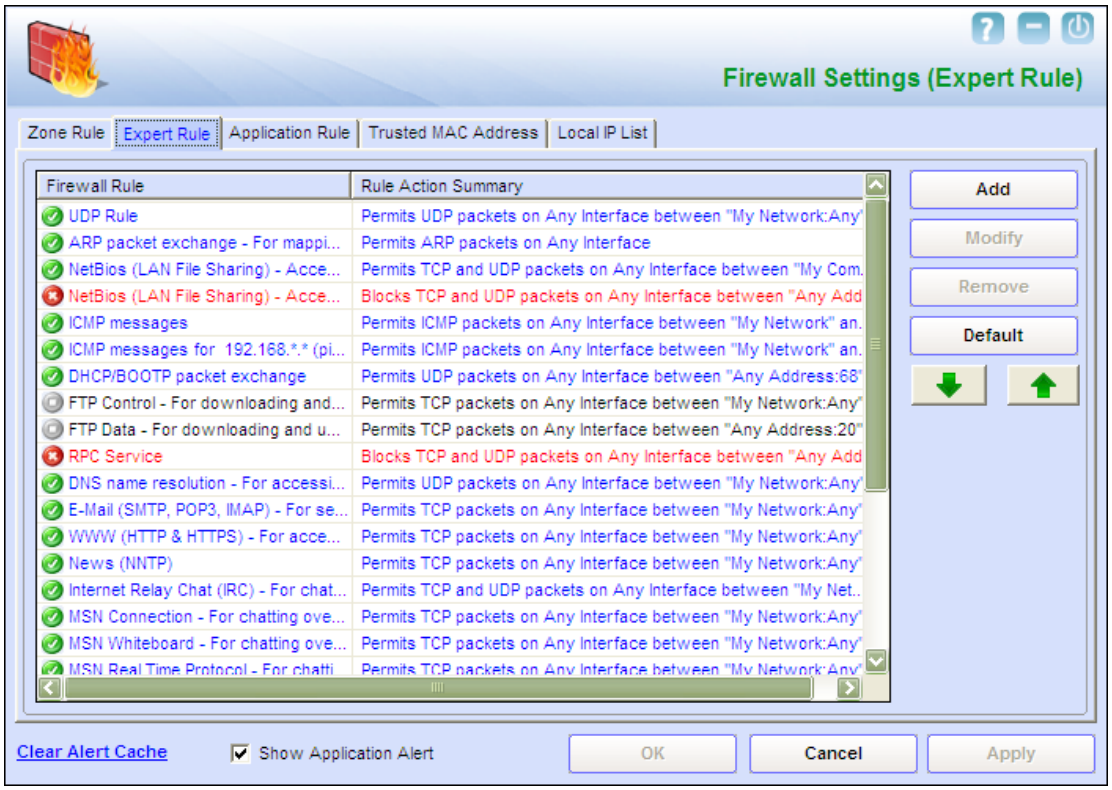
- **Add Host Name:** You can click this button to add a zone rule for a given host. To add the zone rule, you must provide the name of the host for which you

are adding the zone rule; the type of zone, whether it is Trusted or Blocked; and specify a name for the zone rule.

- **Add IP:** You can click this button to add a zone rule for a given IP address. To add the zone rule, you must provide the IP address for which you are adding the zone rule, the type of zone, whether it is Trusted or Blocked; and specify a name for the zone rule.
- **Add IP Range (New Zone):** You can click this button to add a zone rule for a range of IP addresses. To add the zone rule, you must provide the range of IP address for which you are adding the zone rule, start IP address in the range, end IP address in the range; the type of zone, whether it is Trusted or Blocked; and specify a name for the zone rule.
- **Modify:** You can click this button to modify the zone rules related to the host name, IP address, or range of IP addresses. You can also perform these tasks by right clicking the table or row within the table, and then choosing the appropriate option from the context menu.

2. Expert Rule

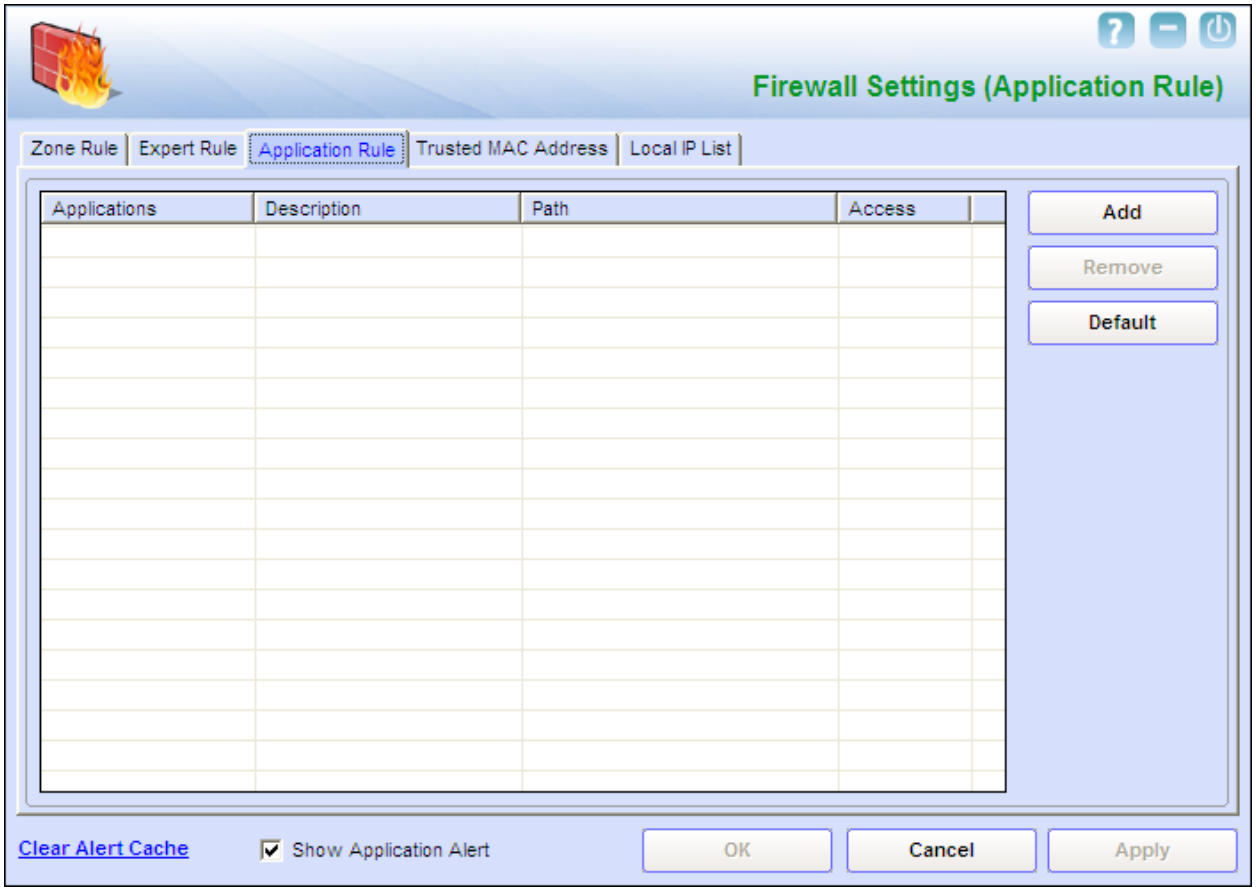
This tab allows you to specify advanced rules and settings for the eScan firewall. You can configure expert rules on the basis of the source IP address or host name, source port number, destination IP address or host name, and destination port number. You can create new expert rules. However, you should configure these rules only if you have a good understanding of firewalls and networking protocols.


Firewall Settings (Expert Rule)
Zone Rule
Expert Rule
Application Rule
Trusted MAC Address
Local IP List
Firewall Rule
Rule Action Summary
UDP Rule
Permits UDP packets on Any Interface between "My Network:Any"
ARP packet exchange - For mappi...
Permits ARP packets on Any Interface
NetBios (LAN File Sharing) - Acce...
Permits TCP and UDP packets on Any Interface between "My Com...
NetBios (LAN File Sharing) - Acce...
Blocks TCP and UDP packets on Any Interface between "Any Add...
ICMP messages
Permits ICMP packets on Any Interface between "My Network" an...
ICMP messages for 192.168.*.* (pi...
Permits ICMP packets on Any Interface between "My Network" an...
DHCP/BOOTP packet exchange
Permits UDP packets on Any Interface between "Any Address:68"...
FTP Control - For downloading and...
Permits TCP packets on Any Interface between "My Network:Any"...
FTP Data - For downloading and u...
Permits TCP packets on Any Interface between "Any Address:20"...
RPC Service
Blocks TCP and UDP packets on Any Interface between "Any Add...
DNS name resolution - For accessi...
Permits UDP packets on Any Interface between "My Network:Any"...
E-Mail (SMTP, POP3, IMAP) - For se...
Permits TCP packets on Any Interface between "My Network:Any"...
WWW (HTTP & HTTPS) - For acce...
Permits TCP packets on Any Interface between "My Network:Any"...
News (NNTP)
Permits TCP packets on Any Interface between "My Network:Any"...
Internet Relay Chat (IRC) - For chat...
Permits TCP and UDP packets on Any Interface between "My Net...
MSN Connection - For chatting ove...
Permits TCP packets on Any Interface between "My Network:Any"...
MSN Whiteboard - For chatting ove...
Permits TCP packets on Any Interface between "My Network:Any"...
Add
Modify
Remove
Default
Clear Alert Cache
Show Application Alert
OK
Cancel
Apply

The Expert Rule Tab

3. Application Rule

An application rule is based on programs or applications that are allowed to or denied access to the Internet or any network-based service. The **Application Rule** tab provides you with a default list of rules and options for configuring application rules. While adding a new application rule, you must provide the path of the application for which the rule is to be applied and to specify whether the Firewall module should allow the application to run.



The Application Rule Tab

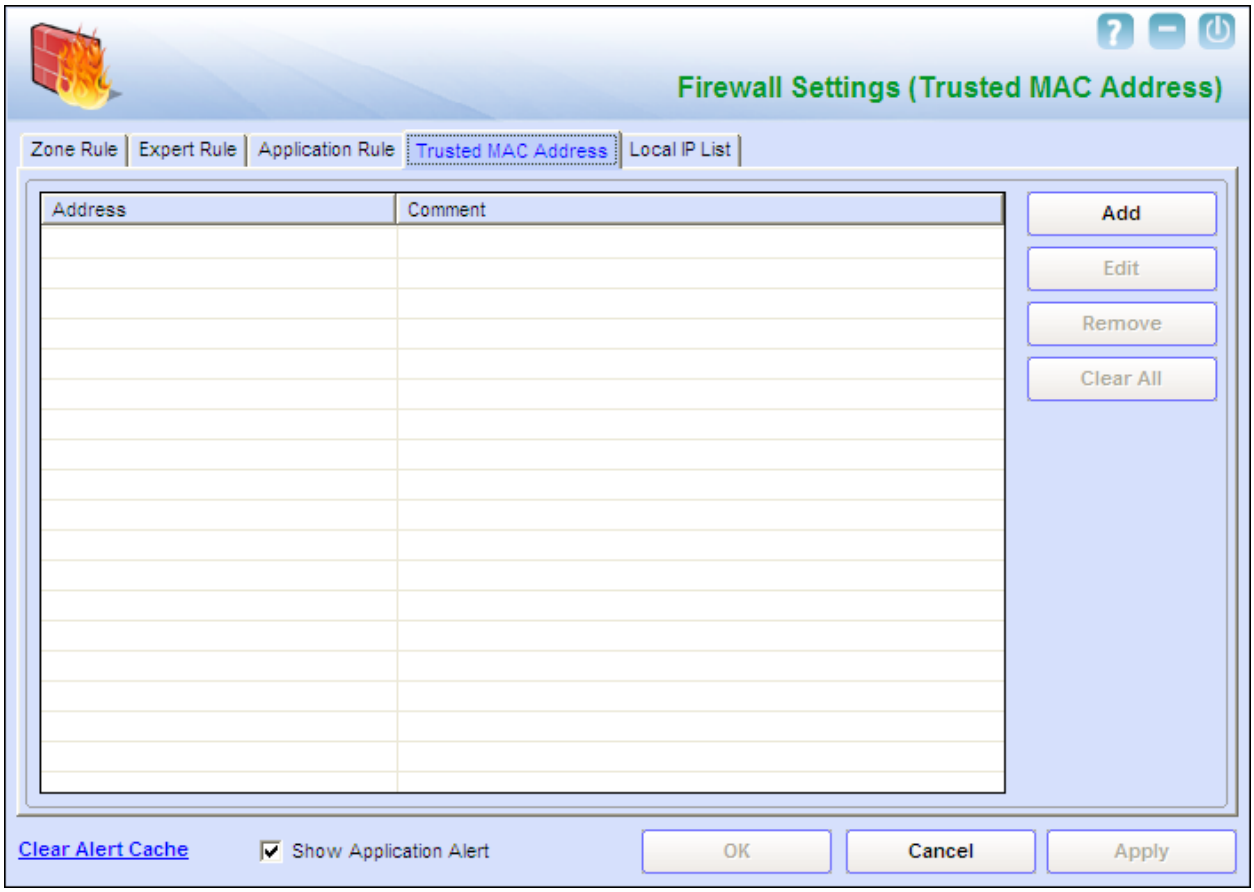
The context menu shows the following additional options when you right click any rule in the table.

- **Process Properties:** This option displays the properties of the selected process or file, which include the name of the file, owner of the file, copyright information, version, and path of the file.
- **Process Details:** This option displays the details of the selected process or file in a browser window. This information is available on the MicroWorld Web site.

4. Trusted MAC Address

This tab contains the information on the MAC addresses of devices connected to the computer. A MAC address is a hardware address that uniquely identifies each node of a network. The Trusted MAC address list is checked along with the expert rule only when **The packet must be from/to a trusted MAC address**

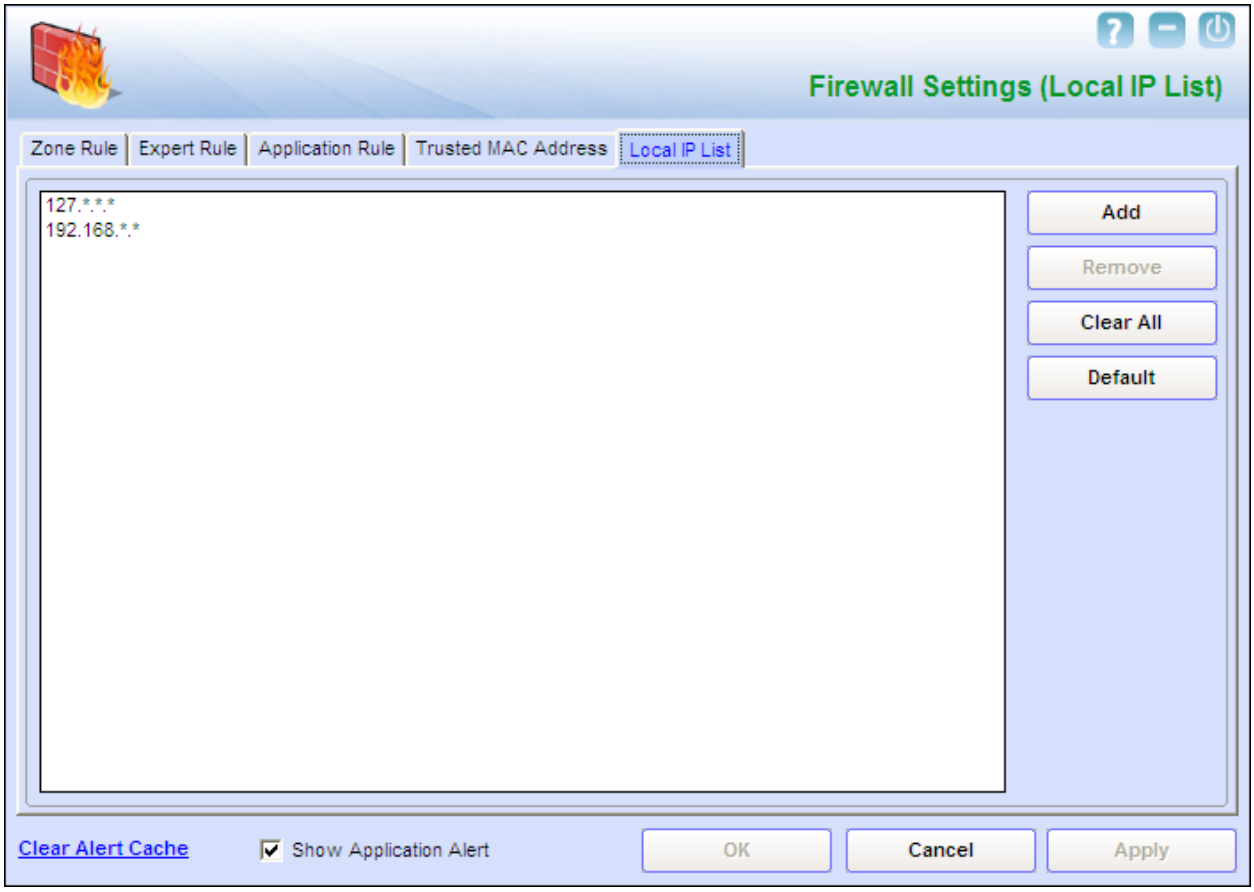
option is selected in the **Add Firewall Rule** dialog box and the action is as per the action specified in the rule.



The Trusted MAC Address Tab

5. Local IP List

This tab contains the list of all the local IP addresses.



The Local IP List Tab

The other options available in this dialog box are as follows:

- **Clear Alert Cache:** You can click this link to clear all the information such as previous actions taken or blocked programs stored in the firewall's cache.
- **Show Application Alert:** This option displays a firewall alert when an application is blocked as per an application rule.

❑ Reports

This section displays the following information.

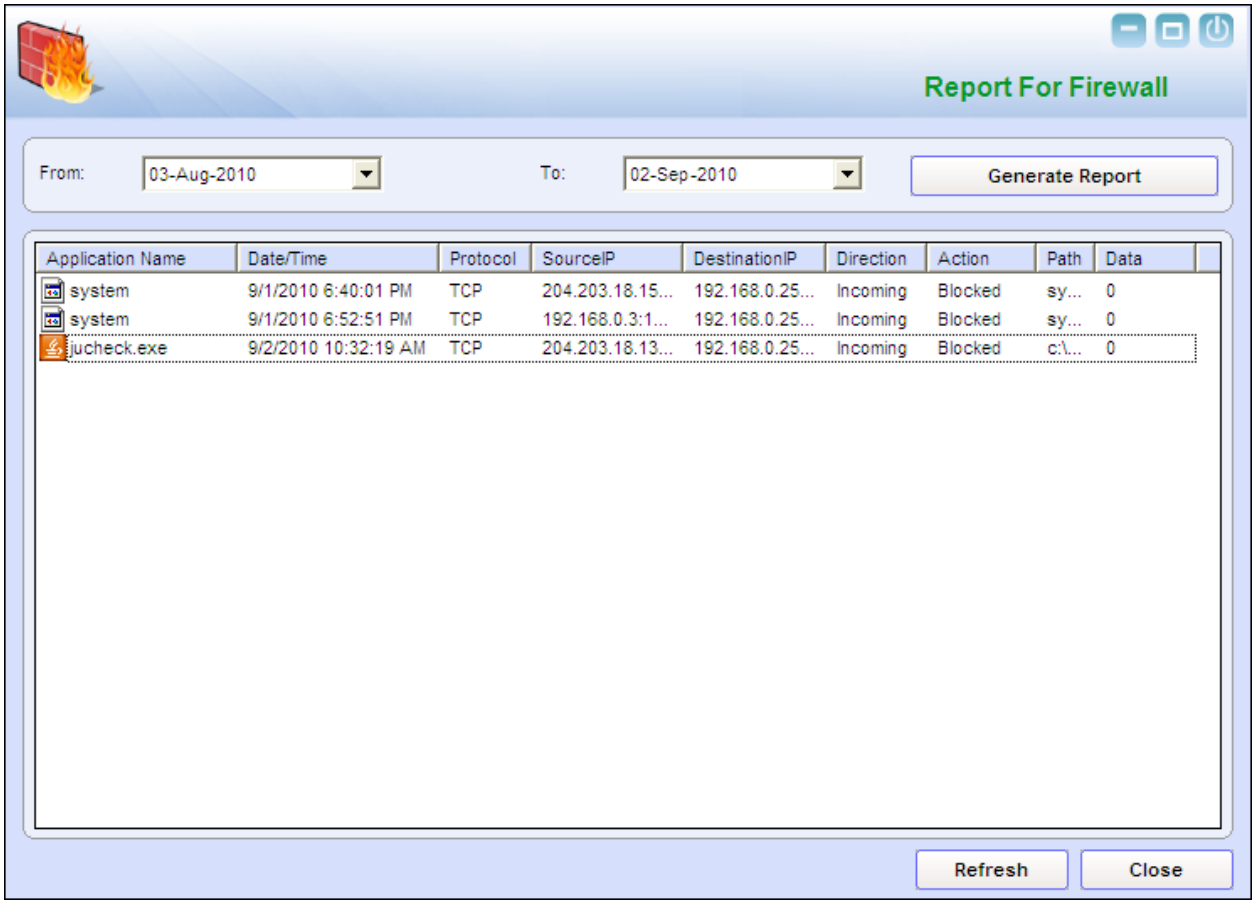
- **Inbound Packets Allowed:** It shows the total number of inbound packets that were allowed by the firewall.
- **Outbound Packets Allowed:** It shows the total number of outbound packets that were allowed by the firewall.

- **Inbound Packets Blocked:** It shows the total number of inbound packets that were blocked by the firewall.
- **Outbound Packets Blocked:** It shows the total number of outbound packets that were blocked by the firewall.

The report section also shows a Network Traffic Monitor, which displays the incoming and outgoing network traffic in Kilobytes per second (KBps).

In addition, you can view the following reports.

- **View Current Network Activity:** You can click this button to open the ViewTCP tool, which displays the real-time activity report of the all active connections and established connections. It also provides you with information regarding the process, protocol, local address, and the remote address and the status of each network connection.
- **View Summary:** You can click this button to view the firewall report either in the form of detailed report or a summary report. A summary report displays information regarding the rules that has been invoked and applied by the firewall. These rules may include application rules, expert rules, zone rules, and Trojan rules. A detailed report includes information about the rules regarding the network activities and shows data in the form of graphs and charts.
- **View Report:** You can click this button to open the **Report for Firewall** window. This window displays the report for the Firewall module for a given range of dates in a tabular format when you click the **Generate Report** button.



The Report For Firewall Window

Scan

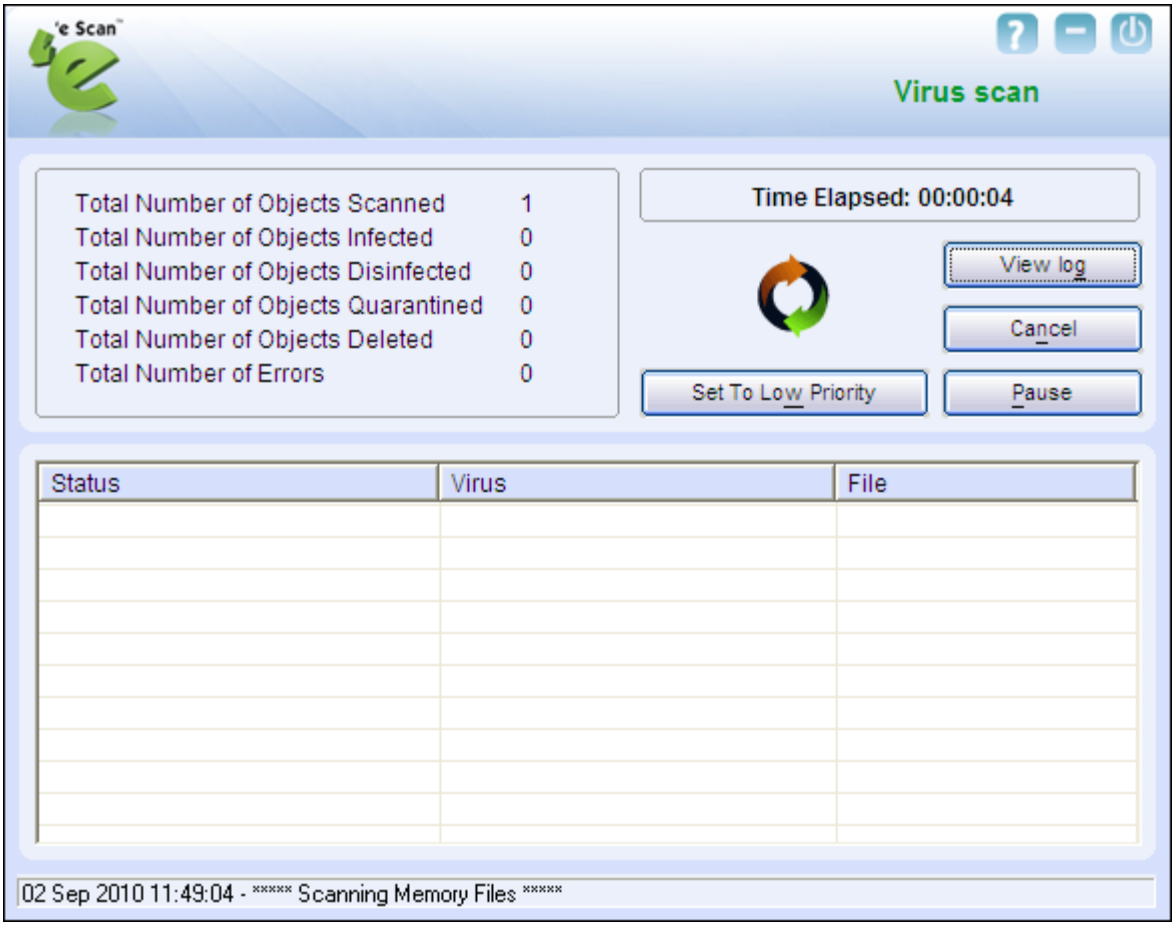
The Scan module helps you perform on-demand scans on files, folders, storage devices, and the registry and schedule automatic scans. It checks your computer for security threats, such as viruses, spyware, and other malicious software and creates logs of all scan operations.

Scan

When you click the Scan button on the eScan Protection Center, the Scan tabbed page is displayed. This page provides you with options for scanning the computer and peripheral storage devices, configuring the Scan module, and scheduling scans.

The **Virus scan** dialog box contains options for scanning the memory, drives, peripheral storage devices, registry, and services running on the computer for viruses and other malware. It displays information about the total number of objects that have been

scanned, infected, disinfected, renamed, and deleted; total number of errors; and time elapsed since the beginning of the scan. In addition, it provides you with the option of running scans as low-priority processes. After you have finished scanning the computer, you can view the log files by clicking the **View log** button.



The Virus scan Dialog Box

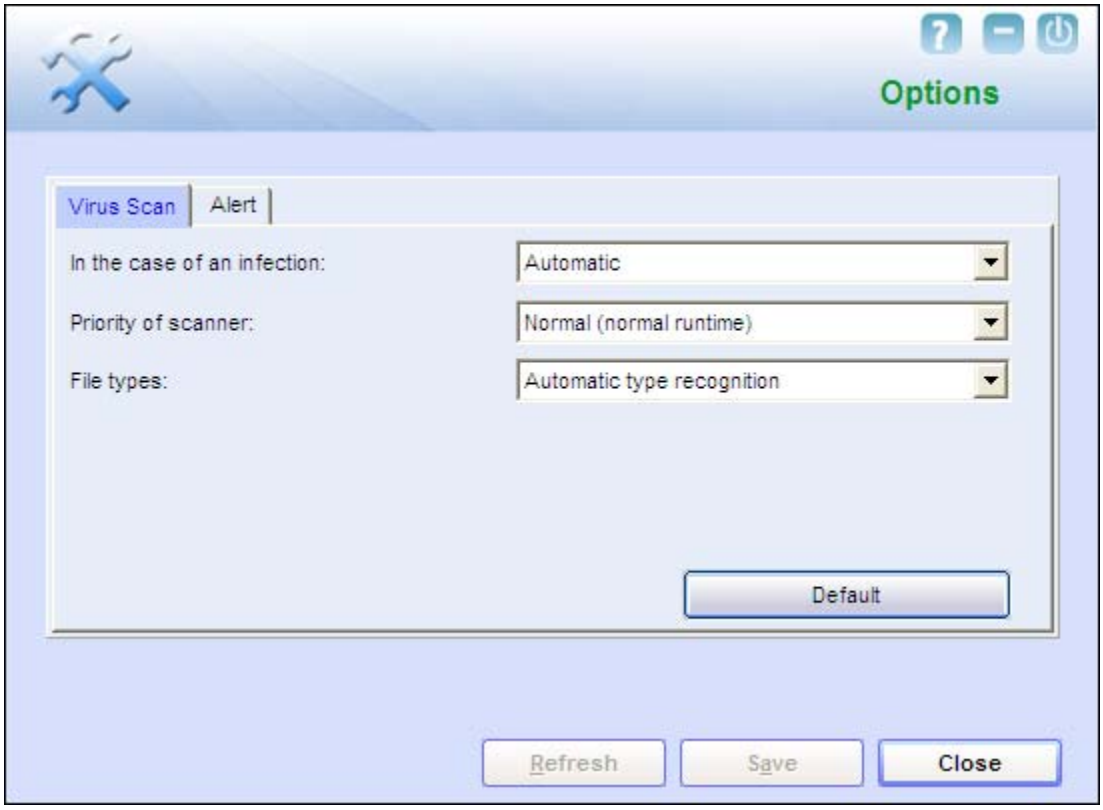
You can click the **Custom Scan Options** dialog box to perform customized scans by configuring eScan to scan the selected storage devices or objects for malicious software. This dialog box provides you with several scan options, such as **Scan spyware; Check memory, registry and services; Scan USB drives, Scan startup,** and **Check local hard drives.** In addition, you can select the **Check following directories and files option** to scan specific files and folders for malware.

In addition, the Scan tabbed pane shows the following buttons.

- **Options.** You can configure **Scan** options by clicking the **Options** button. This will display the **Options** dialog box, which provides you with options for configuring the Scan module. This dialog box has two panes: Virus Check and Alert.

1. Virus Scan

This tab helps you configure the actions that eScan should perform when an infection is detected. It allows you to set the priority of the scan process as **High, Normal,** or **Low.** It also helps you configure eScan to automatically recognize either all file types or only program files.



The Virus Scan Tab

- **In the case of an infection:** This list helps you configure the action that eScan should perform on the file when it finds that it is infected. The actions are as follows:

  - **Log only:** When you select this option, eScan only logs the occurrence of the virus infection without taking any action.

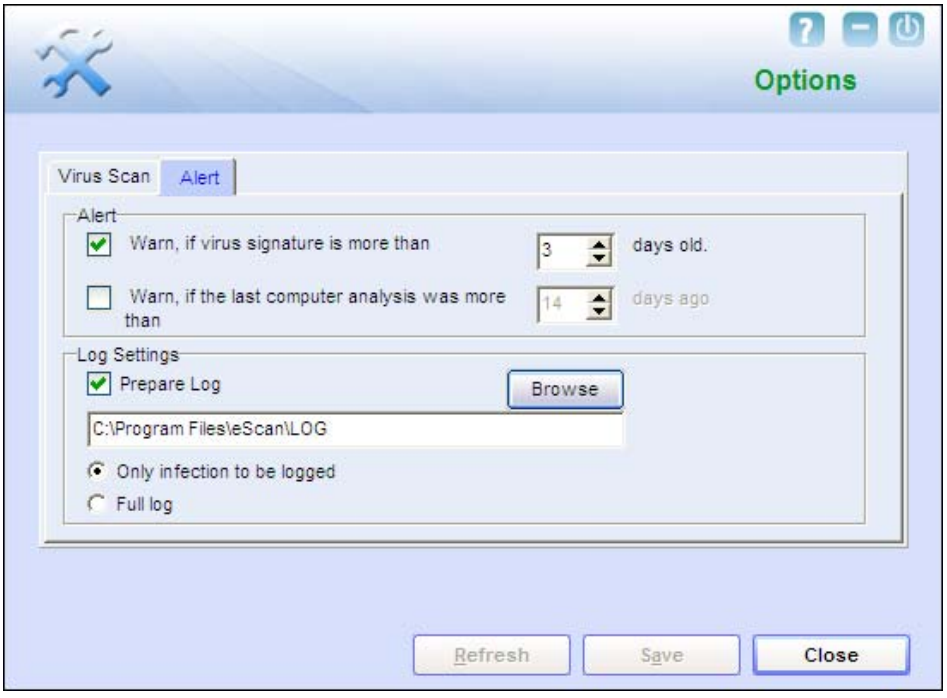
- **Delete infected file:** When you select this option, eScan deletes the infected file.
- **Automatic:** [Default] When you select this option, eScan first tries to clean the file. If it is not possible to disinfect the file, eScan quarantines or deletes the file.

- **Priority of scanner:** This option helps you set the priority of the eScan scanner in relation to other processes running on the computer. The priority level can be high, normal, or low. By default, the scanner runs with low priority.
- **File types:** This option helps you select the type of files that should be scanned by On-demand Scan.

  - **Automatic type recognition:** [Default] When you select this option, On-demand Scan will scan all files but will ignore files that cannot be infected.
  - **Only program files:** When you select this option, On-demand Scan will scan only the program files or executables stored on your computer.

2. Alert

This tab helps you configure eScan to alert you when it detects malicious software on your computer.



The Alert Tab

- **Alert:** In this section, you can configure when eScan should notify you when the virus definitions are outdated or when a specified number of days have elapsed since you have last scanned your computer.

  - **Warn, if virus signature is more than:** [Default] When you select this check box, eScan will notify you if the virus signature is older than the specified number of days. By default, eScan notifies you when your virus definitions are more than three days old.
  - **Warn, if the last computer scan was more than:** When you select this check box, eScan will notify you when a specified number of days have elapsed since the computer was last scanned.

- **Log Settings section:** In this section, you can configure the log settings for the Scan module.

  - **Prepare log:** [Default] When you select this check box, eScan creates an On-demand Scan log file at the specified path. The default path is c:\Program Files\eScan\LOG.
  - **Only infection to be logged:** [Default] When this option is selected, eScan will log information only about infected files and the action taken on them in the On-demand Scan log.
  - **Full log:** When this option is selected, the On-demand Scan log will contain information about all the files scanned by eScan.

- **Scheduler:** In this section, you can schedule On-demand Scan to scan your computer and storage devices for malicious objects. It contains a table, which displays the name of the schedule, the frequency of occurrence, and the next time it will be run. This dialog box includes an **Add task** button, which helps you add a new scan task to the schedule.

  - **Add task:** When you click this button, eScan opens the **Automatic virus scan** dialog box. This dialog box includes the **Job**, **Analysis extent**, **Schedule**, and **Virus check** tabs.

    - **Job:** This tab helps you specify the name, start type, and termination condition for a new task. If you select the start type as **Start in foreground**, the task will run in the foreground, otherwise, the task will run in the background and its window will be minimized. You can also

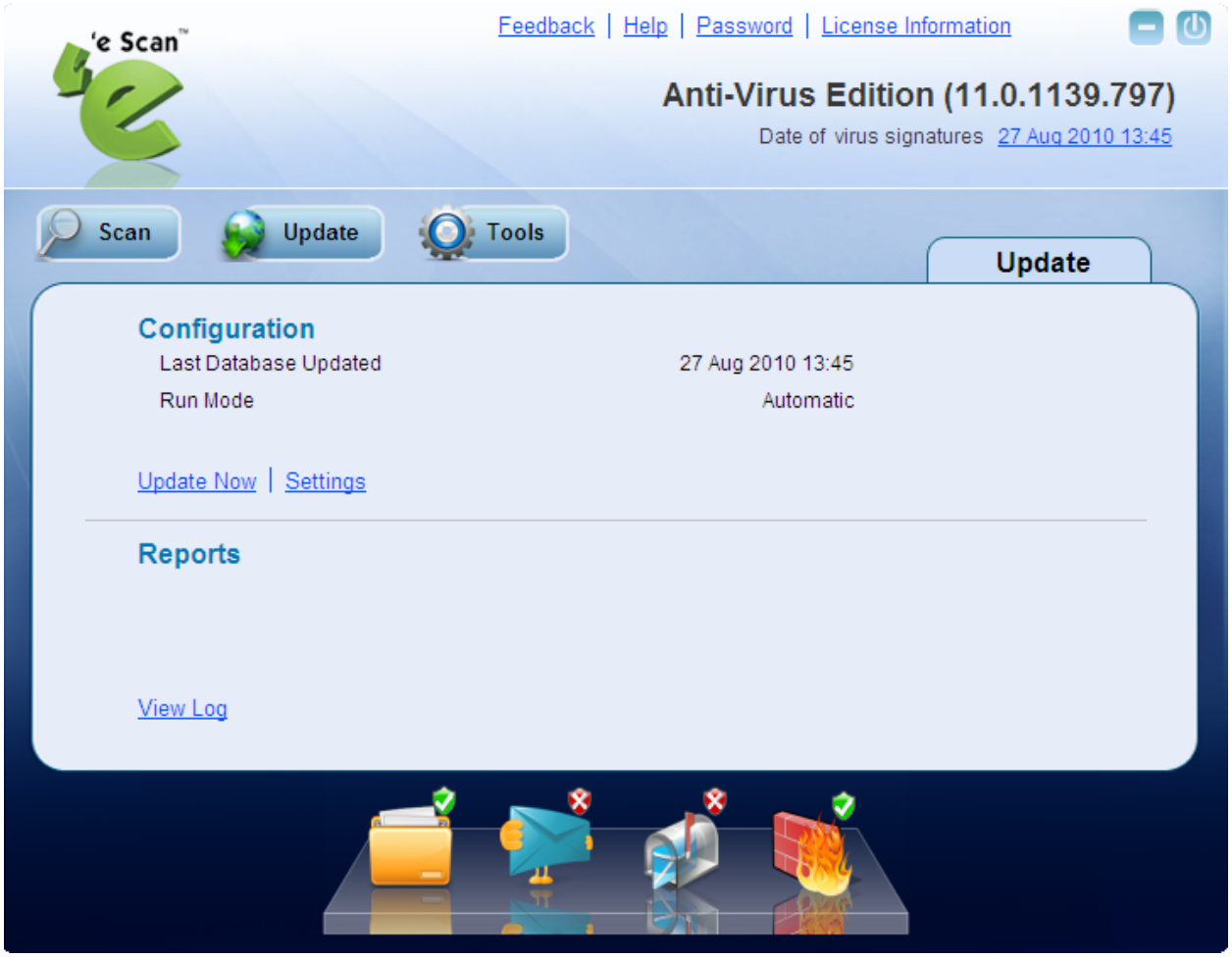
select the termination condition for the task. For example, you can specify that the On-demand Scan should always quit automatically after it has finished scanning.

- **Analysis extent:** This tab presents you with options that help you select the type of scanning, and the directories, folders, or local hard drives to be scanned.
- **Schedule:** This tab helps you configure the options for scheduling system scans. You can schedule scans to run either once or on a daily, hourly, weekly, monthly basis, when the computer boots up, or on a given date at a specific time.
- **Virus check:** This tab provides you with the same options as the ones present on the **Virus Check** tab of the Scan module. You can configure On-demand Scan to perform a specific action when a virus infection is detected. You can also set the priority of the eScan scanner in relation to other processes running on the computer. The priority level can be high, normal, or low. By default, the scanner runs with low priority. In addition, you can configure On-demand Scan to scan only program files or executable files.

- **Logs:** You can view the reports of the scheduled On-demand Scan scans performed on your computer and storage devices in the **Logs** dialog box.

Update

The Update module automatically keeps your virus definitions up-to-date and protects your computer from emerging species of viruses and other malicious programs. You can configure eScan to download updates automatically either from eScan update servers or from the local network by using FTP or HTTP.



Update

You can access the tabbed page for the Update module from the Protection Center by clicking the **Update** button. The **Update** tabbed page provides you with information regarding the mode of updation and date on which the database was last updated. It also provides you with options for configuring the module and helps you view reports on the recent scans performed by the module.

The tabbed page shows two sections: Configuration and Reports. These two sections are described as follows:

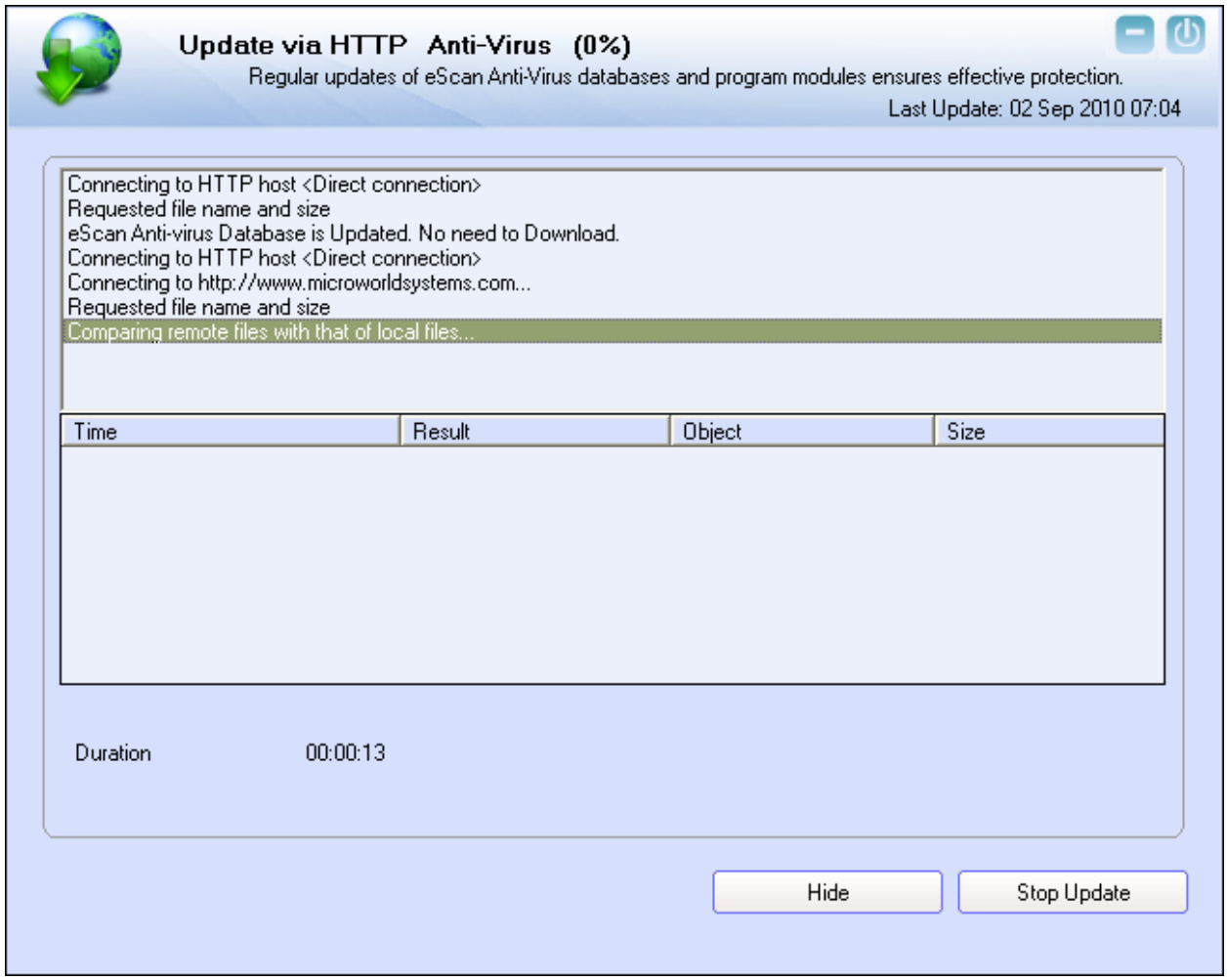
❑ Configuration

This section displays the following information.

- **Last Database Updated:** It shows when the eScan database was last updated.
- **Run Mode:** It displays mode of updation used by eScan. The run mode can be either Automatic or Scheduled.

In addition, you can click any one of the following buttons.

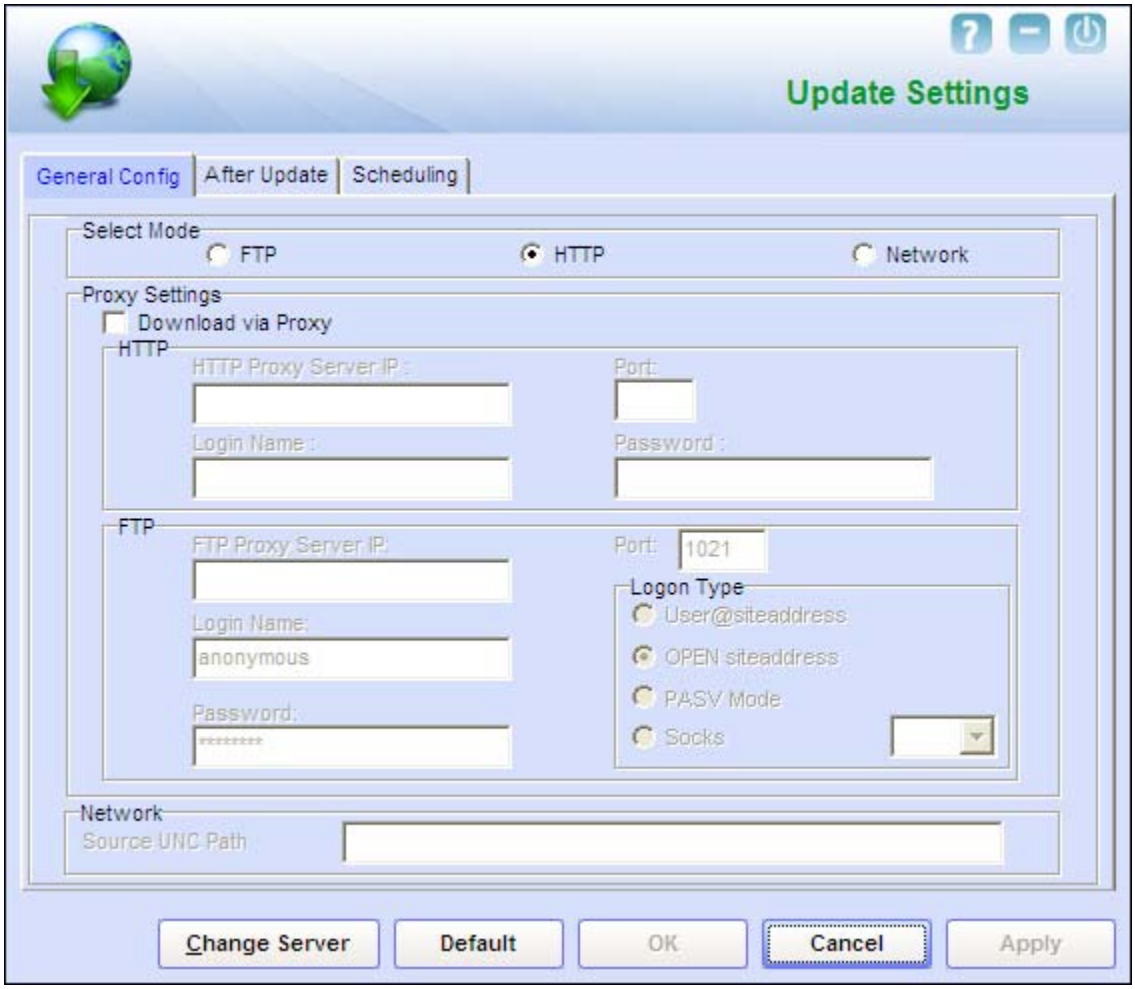
❑ **Update Now:** You can click this button to update the Anti-Virus and Anti-Spam definitions via HTTP, FTP, or Network mode.



- **Settings:** You can click this button to open the **Update Settings** dialog box, which helps you configure the Update module to download updates automatically. This dialog box has the following tabs.

1. General Config

This tab provides you with general options for configuring the Updater module.



The General Config Tab

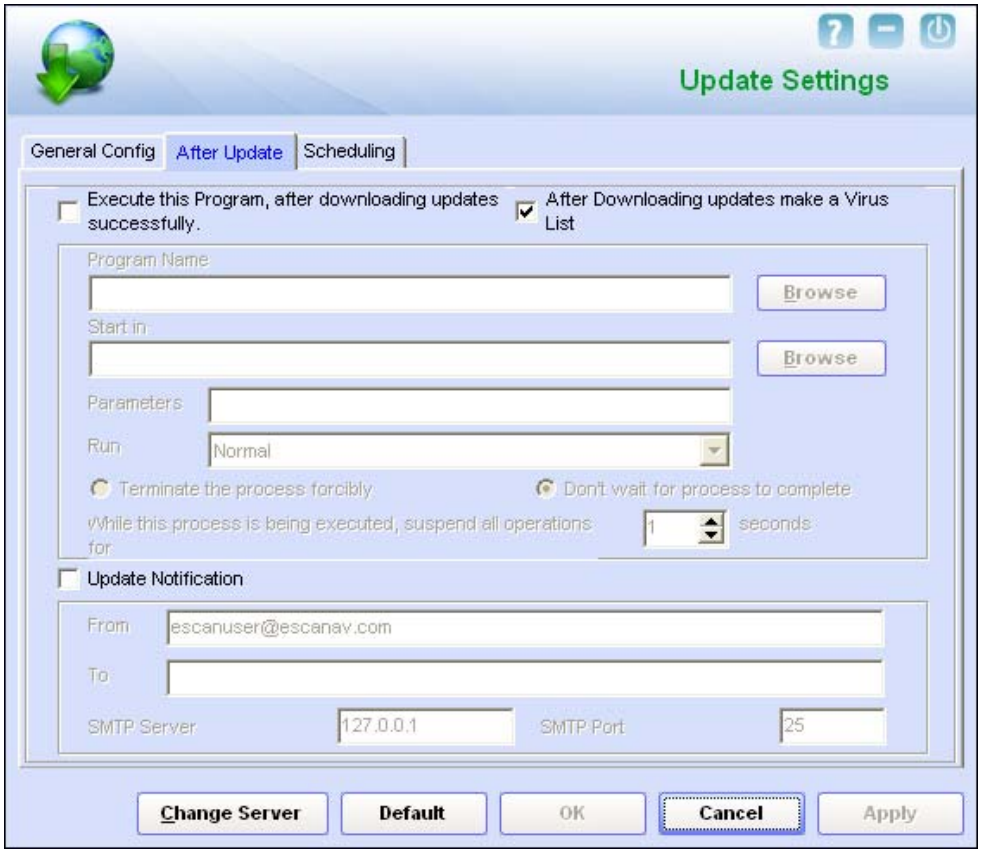
- **Select Mode:** You can select the mode for downloading updates from eScan update servers. The available modes are **FTP**, **HTTP**, and **Network**.
- **Proxy Settings:** In this section, you can configure the proxy settings for downloading updates via HTTP proxy or FTP proxy servers. In both case, you need to provide the IP address of the server, the port number, and the

authentication credentials. In case of FTP servers, you also need to provide the format for the user id in the **Logon Type** section.

- **Network:** This section is enabled when you select the **Network** mode for downloading updates. You must specify the source UNC path in this section.

2. After Update

This tab helps you configure the actions that eScan should perform after Updater downloads the updates.



The After Update Tab

- **After Downloading updates make a Virus List:** [Default] When you select this check box, eScan automatically creates a virus list after the updates are downloaded successfully.
- **Execute this Program, after downloading updates successfully:** When you select this check box, eScan runs a particular application or program after eScan updates are downloaded successfully.

This section shows the following options.

- **Program Name:** Sometimes, you may need a particular program to run after you have downloaded updates for eScan. You can simply specify the path of the program in the **Program Name** box. Alternatively, you can use the **Browse** button to navigate to the path where the program executable is stored.
- **Start In:** You can also specify the program to execute from a given location. You can either specify the location in the **Start In** box or use the **Browse** button to navigate to the folder where the program should execute.
- **Parameters:** Some programs require additional parameters to execute. You can specify these start parameters in the **Parameters** box.
- **Run:** **[Default: Normal]** Whenever a program runs, it runs in its own window. You can specify whether the window should be in the maximized, minimized, normal, or hidden state. The default state of the window is normal.
- **Terminate the process forcibly:** You can also forcibly terminate the process to free system resources by selecting this option.
- **Don't wait for process to complete:** A process may require a long time to end. In such cases, you can allow other processes to run along with the specified process by selecting this option.
- **While this process is being executed, suspend all operations for <placeholder> seconds:** **[Default: 1]** You can also ensure that the no other process runs while the specified process is running for a given time interval by setting the interval in the box.

Note: The options in the **Execute this Program, after downloading updates successfully** section are disabled by default.

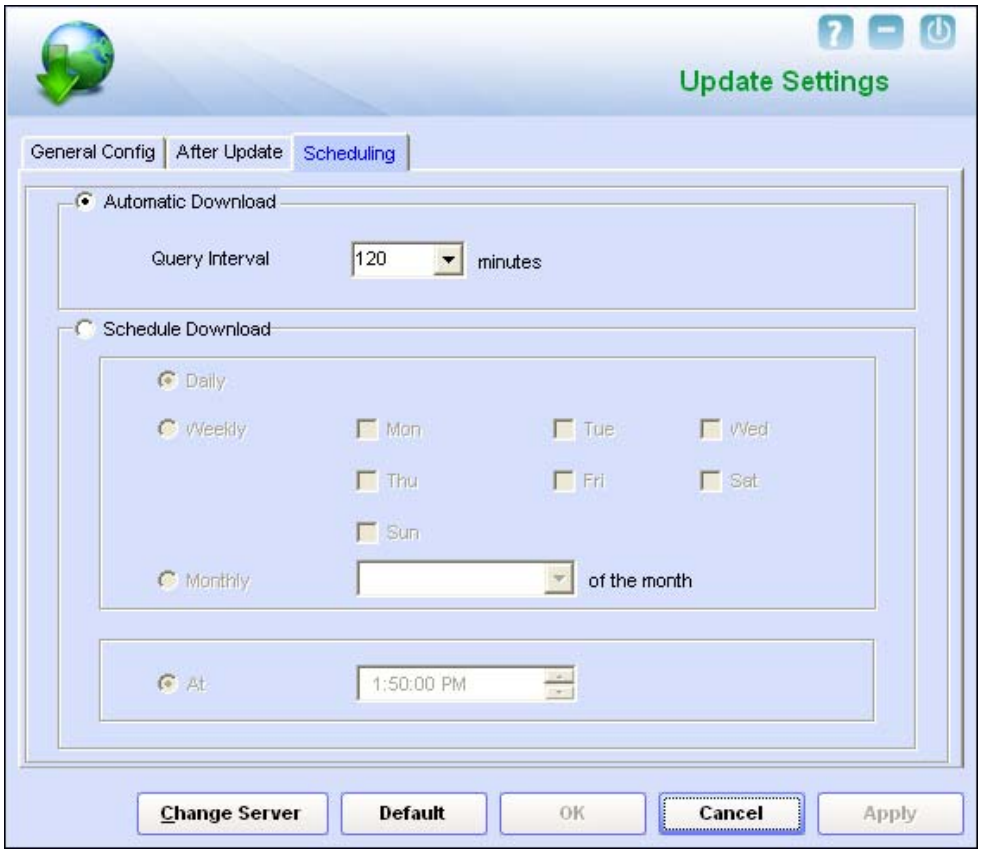
- **Update Notification:** When you select this option, eScan sends an e-mail notification to the e-mail address specified in the **To** box in the **Update Notification** section.

  - **From:** **[Default: escanuser@escanav.com]** You can specify the sender's e-mail address in the notification mail in this box.
  - **To:** You can specify the recipient's e-mail address in the notification mail in this box.

- **SMTP Server:** [Default: 127:0:0:1] You can specify the IP address of the SMTP server in this box.
- **SMTP Port:** [Default: 25] You can specify the port number of the SMTP port in this box.

3. Scheduling

The Scheduler automatically polls the Web site for updates and downloads the latest updates when they are available. You can also schedule downloads to occur on specific days or at a specific time.



The Update Settings Tab

- **Automatic Download:** [Default] You can configure the Update module to query and download the latest updates automatically from the MicroWorld Web site. You can configure the query interval by using the following setting.

  - **Query Interval:** [Default: 120] You can set the interval after which eScan should query the Web site for latest updates.

- **Schedule Download:** **[Default: Daily]** You can also schedule downloads to occur on specific days or on a daily, weekly, or monthly basis. In addition, eScan also provides you with the facility of downloading updates at a specific time. By default, eScan downloads updates at **1:50:00 PM**. When you configure this setting, the Scheduler checks the MicroWorld Web site for latest updates at the specified time and downloads them if they are available.
- **Change Server:** You can click this button to download updates from another eScan server.

❑ Reports

This section displays the following information.

- **View Log:** When you click this link, the View Update Log window is displayed. This window displays the latest activity report for the Update module.

  This report includes the following information.

  - The timestamp, session description, and host name or IP address.
  - The description of the file, such as the result of the download, the name of the object, and its size.
  - The description of the event, such as the number of files downloaded, the time at which the connection was established or terminated, and the errors, if any.

Tools

You can access the **Tools** tabbed page by clicking the Tools button in the eScan Protection Center window. This page provides you with options for sending debug information to the eScan Technical Support Team, creating the eScan rescue image, downloading the latest hotfix, restoring the Windows® default settings, and contacting the eScan Remote Support.

Tools

These options are described as follows:

- **Send Debug Information:** You click this button to open the **Please type your Problem here!** dialog box. This dialog box allows you to specify the eScan-related problem and generate the debuges.zip file. The debuges.zip file is a special file that contains critical eScan files and settings. It is stored in the Program

Files\eScan\Debug folder. You can send the problem description along with the debuges.zip file to eScan's Technical Support Team so that they can analyze it and assist you in resolving the problem.

To send the description of the problem, you need to specify the following information.

- **Mail From:** **[Default: escanuser@escanav.com]** You can specify the e-mail address of the sender in this box.
- **Mail To:** **[Default: support@escanav.com]** You can specify the e-mail address of the recipient in this box. The recipient of this e-mail is usually the eScan's Technical Support Team.
- **SMTP Server:** **[Default: mail.mwti.net]** You can specify the IP address of the SMTP server in this box.
- **SMTP Port:** **[Default: 25]** You can specify the port number of the SMTP port in this box.
- **User Authentication (Opt.):** You can specify the user name in this box, however adding this information is optional.
- **Authentication Password (Opt.):** You can specify the user name in this box, however adding this information is optional.
- **OK:** When you click this button, the e-mail along with the debuges.zip file is sent to eScan's Technical Support team.

- **Create eScan Rescue ISO Image File:** You can click this button to open the eScan Rescue File Creation Wizard, which will help you create a Windows®-based Rescue Disk file. The Rescue Disk file will help you create a clean bootable CD to provide you a clean boot on infected computers running the Windows® operating system. You can then eradicate rootkits and file infectors that cannot be cleaned in the normal Windows® mode.

  For more information on how to create the eScan Rescue Disk file, visit the following link.

  http://escanav.com/documents/escan11/escan_rescue_disk.asp

- **Download Latest Hotfix (eScan):** **[Requires Internet connectivity]** When you click this button, eScan opens the MicroWorld Download Manager and starts downloading the latest hotfix from eScan update servers.
- **Restore Windows Default Settings:** You can restore the Windows® operating settings, such as desktop and background settings, to eliminate all the modifications made by a virus attack by using this button. eScan automatically scans your

computer for viruses when you click this button and sets the system variables to their default values.

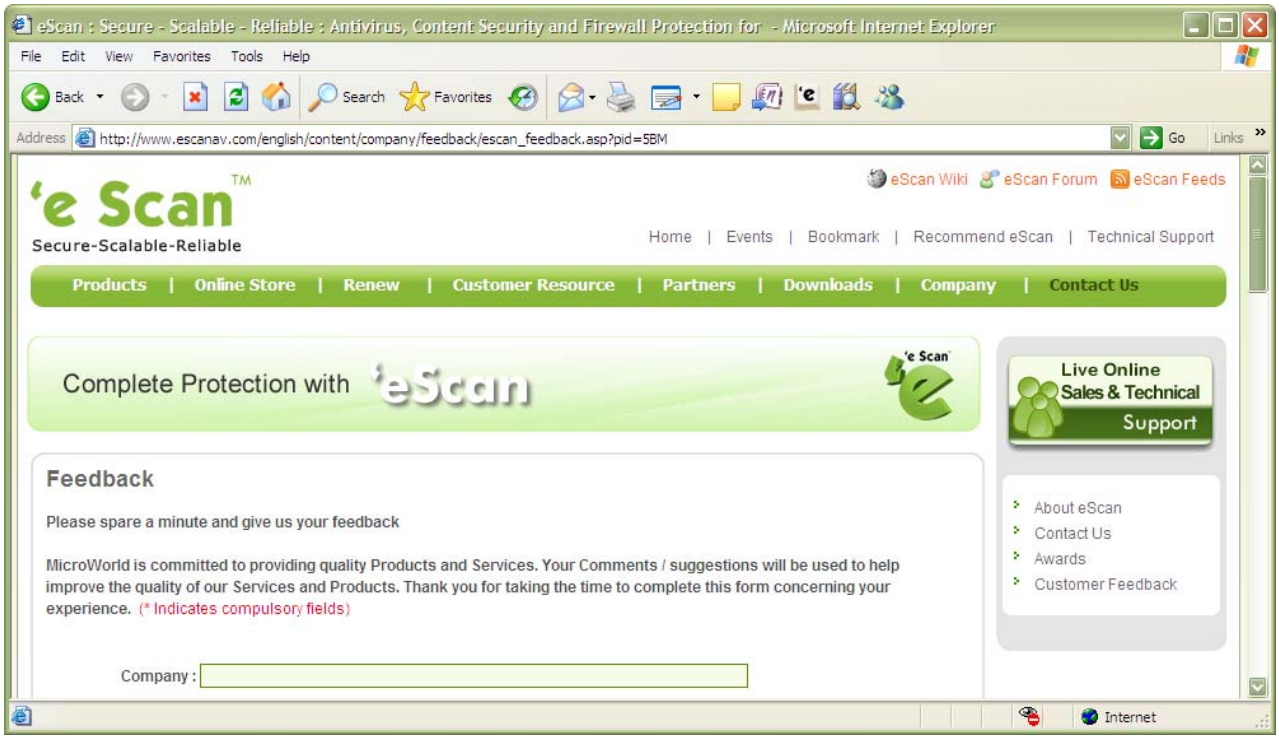
- **Download Latest Hotfix (Microsoft Windows OS):** When you click this hyperlink, eScan opens the MicroWorld Download Manager and starts downloading the latest hotfix for the Windows® operating system from the Microsoft® Web site.
- **eScan Remote Support:** eScan Remote Support works with the help of a special software. This feature helps you request the assistance of an eScan Support Technician. When you click this button, the eScan Remote Support service will start on your computer and you will get a unique user id and a password. You can provide this to the eScan Support Technician to take control of your computer remotely and troubleshoot the eScan-related issues.

  Note: To run eScan Remote Support, your computer should have the latest eScan hotfix installed on it and it should be connected to the Internet.

eScan Protection Center includes the following modules.

Feedback

The Feedback button is displayed on the top right-hand corner of the eScan Protection Center window. You can click this button to visit the eScan Web site, where you can provide your feedback on various eScan products and send it to the eScan's Quality Assurance team.


eScan : Secure - Scalable - Reliable : Antivirus, Content Security and Firewall Protection for - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Back Search Favorites
Address http://www.escanav.com/english/content/company/feedback/escan_feedback.asp?pid=5BM
Go Links
'e Scan™
Secure-Scalable-Reliable
eScan Wiki eScan Forum eScan Feeds
Home | Events | Bookmark | Recommend eScan | Technical Support
Products | Online Store | Renew | Customer Resource | Partners | Downloads | Company | Contact Us
Complete Protection with 'eScan
Live Online Sales & Technical Support
Feedback
Please spare a minute and give us your feedback
MicroWorld is committed to providing quality Products and Services. Your Comments / suggestions will be used to help improve the quality of our Services and Products. Thank you for taking the time to complete this form concerning your experience. (* Indicates compulsory fields)
Company :
About eScan
Contact Us
Awards
Customer Feedback
Internet

Feedback Form

Help

You can access the Help section by clicking the Help button on the top right-hand corner of the eScan Protection Center window. This will open a tabbed page, which contains the Live Chat, eScan Online Help, and the MicroWorld Forum buttons.

- **Live Chat [Requires Internet connectivity]:** You can contact eScan's 24 x 7 online Technical Support team via chat either by clicking the **Live Chat** button or by visiting the following link. http://www.escanav.com/english/livechat.asp.

- **eScan Online Help [Requires Internet connectivity]:** eScan Online Help is located on the MicroWorld's wiki. It provides you with comprehensive information about eScan's products and features.

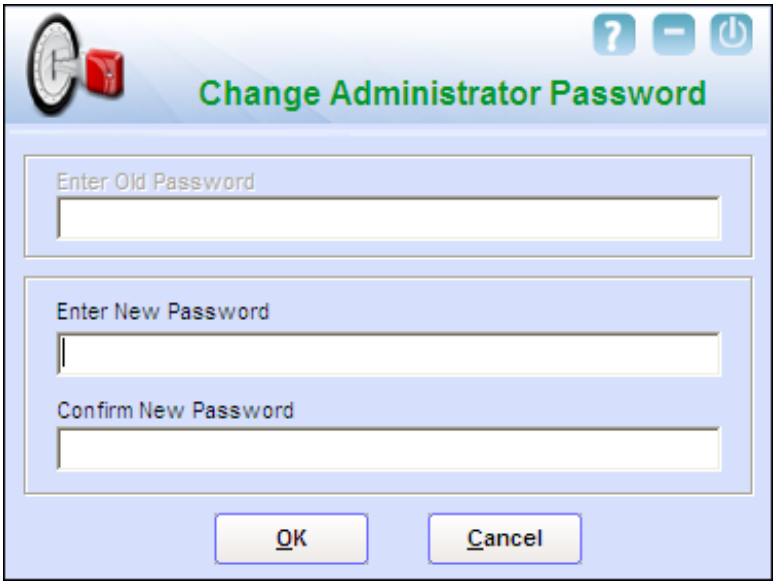
  You can visit eScan Online Help pages either by clicking the eScan Online Help button or by visiting the following link.
  http://www.escanav.com/wiki

  eScan Protection Center also provides you with context-sensitive help. If you need information on a specific feature while viewing the eScan Protection Center window, you can press F1. This will open the relevant page of eScan Online Help.

- **MicroWorld Forum [Requires Internet connectivity]:** You can click this button to join on the MicroWorld Forum and read the discussion threads on eScan.

Password

You can click this button to view the **Change Administrator Password** dialog. You can use this dialog box to change the eScan administrator password for Protection Center.

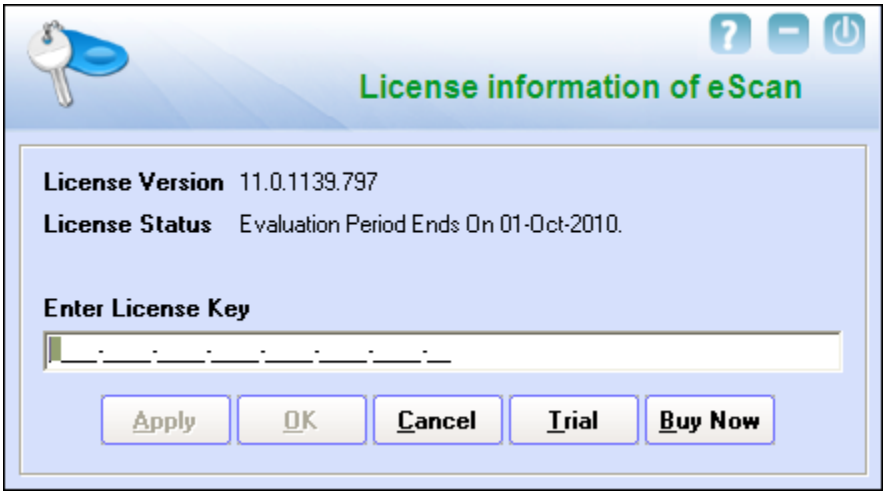


The Change Administrator Password Dialog Box

License

You should register your copy of eScan to prevent others from misusing your license. To do this, you must activate the license key after installing eScan.

You can enter the license key for eScan via the **License information of eScan** dialog box. This dialog box is displayed when you click the **License** button on the top right-hand corner of the eScan Protection Center window.



The License information of eScan Dialog Box

Contact Details

We offer 24x7 FREE Online Technical Support to our customers through e-mail and Live Chat. We also provide FREE Telephonic Support to our customers during business hours.

Chat Support

The eScan Technical Support team is available round the clock to assist you with your queries. You can contact our support team via Live Chat by visiting the following link. **http://www.escanav.com/english/livechat.asp.**

Forums Support

You can even join the MicroWorld Forum at **http://forums.escanav.com** to discuss all your eScan related problems with eScan experts.

E-mail Support

Please send your queries, suggestions, and comments about our products about our products or this guide to **support@escanav.com**

Registered Offices

Asia Pacific
MicroWorld Software Services Pvt. Ltd.
Plot No 80, Road 15, MIDC, Marol
Andheri (E), Mumbai
India

Tel : (91) (22) 2826-5701
Fax: (91) (22) 2830-4750
E-mail : **sales@escanav.com**
Web site: **http://www.escanav.com**

Malaysia
MicroWorld Technologies Sdn.Bhd.
(Co.No. 722338-A)
E-8-6, Megan Avenue 1, 189, Jalan Tun Razak, 50400 Kuala Lumpur
Malaysia

Tel : (603) 2333-8909 or (603) 2333-8910
Fax: (603) 2333-8911
E-mail : **sales@escanav.com**
Web site: **http://www.escanav.com**

South Africa
MicroWorld Technologies South Africa (PTY) Ltd.
376 Oak Avenue
Block C (Entrance from 372 Oak Avenue)
Ferndale, Randburg, Gauteng, South Africa

Tel : Local 08610 eScan (37226)
Fax: (086) 502 0482
International : (27) (11) 781-4235
E-mail : **sales@microworld.co.za**
Web site: **http://www.microworld.co.za**

USA
MicroWorld Technologies Inc.
33045 Hamilton Court East, Suite 105
Farmington Hills, MI 48334-3385
USA

Tel : (1) (248) 848 9081
Fax: (1) (248) 848 9085
E-mail : **sales@escanav.com**
Web site: **http://www.escanav.com**

Germany
MicroWorld Technologies GmbH
Leopoldstr. 244
D-80807 Munich
Germany

Tel : (49) (0) 89 20 80 39-223
Fax: (49) (0) 89 20 80 39-226
E-mail : **sales@escanav.de**
Web site: **http://www.escanav.de**